Роман Викторович Душкин
Математика и криптография. Тайны шифров и логическое мышление



«Роман Душкин. Математика и криптография : тайны шифров и логическое мышление»: АСТ; Москва; 2018

ISBN 978-5-17-096808-4

Аннотация

Хочешь научиться хранить свои тайны, создавать зашифрованные послания и удивлять одноклассников познаниями в криптографии – науке о создании, использовании и взломе шифров? В этой книге тебя ждёт знакомство с тайными знаниями и умениями, которые доступны только избранным – шпионам, секретным агентам, учёным. Вместе мы научимся кодировать сообщения, используя разные методы шифровки, разгадывать уже существующие тайные послания, делать шифровальные машины и даже создавать свои

оригинальные шифры и загадки!

У тебя есть уникальная возможность познакомиться с реальным миром тайных агентов и спецслужб, ведь все методы шифрования, описанные в книге, используются до сих пор! А вдруг ты сможешь создать свой уникальный метод шифровки?

Роман Душкин
Математика и криптография: тайны шифров и логическое мышление

Введение

Приветствую тебя, уважаемый читатель!

В этой книге я хотел бы посвятить тебя в некоторые тайные знания и умения, обычно доступные только избранным – шпионам и тайным агентам, пиратам и первооткрывателям дальних стран и, конечно же, учёным. Мы научимся писать зашифрованные послания и расшифровывать тайные записи (то есть разгадывать чужие секреты). Мы узнаем немало нового о том, как секретные умения развивались со временем и к какому состоянию криптография пришла сейчас. Ведь криптография – наука о создании, использовании и взломе шифров – одна из интереснейших и самых таинственных наук.

Мы пройдём с тобой по страницам книги, и ты узнаешь, как можно закодировать сообщение так, чтобы его практически никто не смог прочесть (а если кто и захотел бы, то на расшифровку ему бы потребовалось столько времени, сколько лет всей Вселенной). Также ты узнаешь, как разгадывать чужие сообщения и узнавать содержание тайных посланий. Конечно, расшифровать можно не любой код, но уверяю, что большинство шифров, которыми пользуются простые люди, например твои одноклассники, расшифровываются практически сразу же (если одноклассники ещё не прочитали эту книгу).

Чтобы с пониманием читать эту книгу и успешно применять методы, которые в ней описаны, желательно, что называется, дружить с математикой – иначе тебе будет непросто понимать описание некоторых способов шифрования и их расшифровки. Ещё лучше, если у тебя есть навыки программирования: тогда многие методы шифрования и расшифровки можно сразу же запрограммировать на компьютере, а не делать всё это вручную. Впрочем, книга написана так, чтобы можно было обойтись и без использования компьютера и языков программирования.

Если на летних каникулах ты прочтёшь эту книгу и выполнишь задания из неё, у тебя, мой уважаемый читатель, останутся не только знания и умения, но и множество интересных и полезных вещиц, вроде таблиц частотности символов и специальных матриц для кодирования перемешиванием. Всё это станет твоим криптографическим багажом, который ты должен беречь как зеницу ока и даже держать его существование в тайне. Ведь один из методов **криптоанализа** (так по-научному называется расшифровка – в противоположность криптографии) – немудрёный шпионаж и кража инструментов для шифрования, паролей и кодов. Целые государства рушились из-за этого, многие войны были проиграны из-за незадачливых шифровальщиков, которые не уделяли должного внимания тайне своей переписки.

Если у тебя есть брат или сестра примерно одного с тобой возраста, то вы можете читать эту книгу вместе и сообща решать загадки, которые вы найдёте на её страницах. Вряд ли вам стоит соревноваться друг с другом. К тому же вы сразу же сможете использовать описанные методы для передачи тайных посланий. Но не забудьте, что в этом деле очень важна секретность. Можно привлекать к этой игре и друзей. Единственное, от чего я хочу

предостеречь, так это от попыток заниматься криптографией с теми, кому еще не исполнилось десять лет. Они просто могут не понять игры, и она будет им неинтересна.

В Интернете есть различные дополнительные материалы к этой книге, так что ты сможешь найти описания новых методов шифрования, программы для создания паролей и ключей и другие полезные штуки для занятия криптографией. Впрочем, прочитав эту книгу, ты поймёшь, что пользоваться чужими наработками можно только с очень большой осторожностью. В закрытых программах или методах могут оказаться так называемые «прослушки» (или «ловушки», или, как говорят программисты, «закладки»), включённые туда разработчиком. Другими словами, разработчик оставляет для себя возможность разгадать твои секреты, а у тебя при этом нет возможности понять, как работает закрытая программа. Ну а если ты пользуешься чужими ключами для шифровки своих тайн, то не удивляйся, если они в конце концов перестанут быть тайнами.

Давай же сделаем первый шаг в мир загадок и шифров.

Неделя 1. Простой шифр подстановки

Ну что ж, начать, пожалуй, нужно с самого простого. Давай разберёмся, что такое шифр.

Шифрование – это метод сокрытия и раскрытия смысла посланий. Сейчас ты читаешь этот текст и понимаешь его смысл. А если бы я не хотел, чтобы любой человек мог понять то, что здесь написано, я бы использовал шифр – например, так: «14 16 13 16 05 06 24 25 20 16 17 16 17 18 16 02 16 03 01 13». Никто кроме меня и тех, кого я посвящу в метод шифровки этого сообщения, не сможет его расшифровать. Другими словами, шифр (или шифровка, или зашифрованное сообщение) – это открытый текст, смысл которого скрыт.

Что значит «*открытый текст* »? Это такой текст, про который понятно, что он есть. Он доступен не только отправителю (автору) и получателю, но и любому другому человеку. Обычно сообщения – как шифрованные, так и нет, – являются открытыми. К примеру, текст этой книги – открытый. Но есть и закрытые тексты, то есть такие, о существовании которых доподлинно знают только отправитель и получатель. Остальные люди могут разве что догадываться о его существовании. О закрытых сообщениях мы поговорим чуть позже.

А что же значит «*скрытый смысл* »? Это значит, что даже если сам текст открыт, понять его могут только отправитель и получатель. Остальные могут попытаться его понять, а при должной сноровке и знаниях раскрыть скрытый смысл, расшифровав послание. А вот обычный, нешифрованный текст имеет открытый смысл – он понятен всем, кто владеет языком, на котором текст написан, и обладает достаточным уровнем знаний для понимания.

Итак, представь себе способ шифрования, когда каждая буква текста заменяется каким-либо символом или числом. Самый простой способ заключается в использовании вместо букв их порядковых номеров. В русском алфавите 33 буквы, так что будут понадобятся числа от 1 до 33. Например, вот так можно зашифровать слово «ШИФР»: 26 10 22 18.

Само собой, это совсем негодный способ шифрования. Боюсь, такой шифр взломает даже тот, кто не читал эту книгу. По крайней мере, большинству людей первым делом придёт в голову попробовать этот способ расшифровки.

Буквы можно заменять и другими буквами. Например, можно воспользоваться правилом «+3»: чтобы зашифровать букву, необходимо взять её номер в алфавите, прибавить к нему «3», а затем использовать букву с полученным порядковым номером. Чтобы зашифровать буквы из конца алфавита, нужно вернуться в начало алфавита, как бы замкнув круг. Это правило позволит зашифровать слово «ШИФР» так: ЫЛЧУ.



Гай Юлий Цезарь. Древнеримский государственный и политический деятель, полководец, писатель. Для передачи секретных сообщений из штаба в войска впервые использовал простой шифр подстановки, сегодня известный как «шифр Цезаря».

Это так называемый «*шифр Цезаря* ». Именно в таком виде Юлий Цезарь использовал его для секретной переписки со своими командирами легионов. Да, в те далёкие времена этот шифр обеспечивал секретность. Но теперь и он не очень хорошо сохраняет тайну, поскольку те, кто хоть немного знает о криптоанализе, мгновенно взломают его (скоро и ты будешь таким человеком).

Наконец, буквы можно заменять на какие-нибудь экзотические значки; их даже можно выдумать самостоятельно. Здесь открывается широкий простор для фантазии. Например, то же слово «ШИФР» в этом случае можно написать бесконечным количеством способов:

ΨΥΞΘ, βƐ↓Ɔ

и т. д. Придумать можно всё что угодно. Однако и в этом случае ни вид символов, ни их сложность не являются защитой – такой шифр можно взломать так же легко, как и в предыдущем варианте.

Честно говоря, я бы вообще не называл *это* шифрованием. С точки зрения математика и программиста это просто смена кодировки. Мы просто используем другие обозначения для тех же самых букв. Это ни на что не влияет с точки зрения защиты сообщения. Подумай хорошенько: если букву «А» всегда заменять одним и тем же другим символом, букву «Б» – каким-то другим символом и так далее, то это отпугнёт только совсем неподготовленных людей, да и то – после первого испуга каждый сможет разобраться, в чём тут дело.

Другими словами, можно вывести такое правило:

Если заменить буквы на какие-либо иные символы, то секретность сообщения не изменится.

Давай посмотрим, как можно взломать такой шифр. Для этого есть несколько методов:

1. *Частотный анализ* символов. Что обозначает этот термин? Одни и те же буквы, какими бы значками они ни обозначались, всегда используются в одном и том же языке с одинаковой частотой. Сейчас ты читаешь этот текст (на русском языке); можно подсчитать количество разных букв, использованных в нем, а потом поделить эти количества на общее число букв. Получатся так называемые *частоты* букв. Так вот эти частоты практически всегда одинаковы для любых текстов, особенно больших.

2. *Подбор и проверка сочетаний* . Иногда можно успешно подобрать слова, если они заведомо используются в зашифрованном тексте. Например, если ты знаешь, что шпион передаёт в свой штаб информацию о новом виде вооружения, то наверняка в тексте найдётся название этого вооружения. «Внимание, штаб! Атакующая сторона намерена использовать рогатки». Если вы с друзьями и впрямь намерены использовать рогатки, то резонно предположить, что где-то в тексте есть это слово.

3. *Наращивание объёма сообщений* . Если шпион передаёт небольшие сообщения, то к ним сложно применить методы частотного анализа, а подбор сочетаний становится иногда делом бессмысленным. В этом случае надо набраться терпения и подождать новых сообщений, которые увеличат объём шифрованного текста. Тогда и можно будет применить оба предыдущих метода.

Эти три метода, используемые вместе или по отдельности, позволяют взломать практически любое сообщение, скрытое *шифром простой подстановки* (именно так называется этот способ шифрования). Но теперь ты можешь понять, как избежать быстрого взлома шифровки. Нужно сделать использование этих трёх методов невозможным. Во-первых, применять такие методы шифрования, которые изменяют частоту символов. Во-вторых, использовать так называемые коды – когда уязвимые для взлома понятия обозначаются специальными словами, кодами. В-третьих, настоящий шпион никогда не использует один и тот же шифр два раза. Никогда!

Об этих методах шифрования мы поговорим позднее. А теперь предлагаю заняться взломом.

Вот, например, тебе пришло письмо, в котором есть такой текст:

[illegible]

Первый взгляд на этот текст заставляет отбросить «это» и заявить, что разгадать его смысл невозможно. Но так ли это? Давай попробуем разобраться.

Выше я уже говорил, что замена символов, которыми обозначаются буквы, не влияет на частоты букв. Именно этим мы сейчас и воспользуемся. Для начала я приведу таблицу, про которую в первую очередь вспоминает всякий уважающий себя криптоаналитик. Вот она:

Буква	Частота %	Буква	Частота %
О	11,08	Ы	1,96
Е, Ё	8,41	Ь	1,92
А	7,92	З	1,75
И	6,83	Г	1,74
Н	6,72	Б	1,71
Т	6,18	Ч	1,47
С	5,33	Й	1,12
Л	5,00	Ж	1,05
Р	4,45	Х	0,89
В	4,33	Ш	0,81
К	3,36	Ю	0,61
М	3,26	Э	0,38
Д	3,05	Щ	0,37
П	2,81	Ц	0,36
У	2,80	Ф	0,19
Я	2,13	Ъ	0,02

О чём эта таблица? В ней указаны частоты встречаемости букв в русском языке в обычных текстах. Как видишь, буква «О» встречается чаще всего. Можно сказать, что каждая десятая буква в тексте на русском языке, – это буква «О». Второе место занимает буква «Е» (вместе с «Ё»). Далее, соответственно, идут буквы «А», «И» и т. д. Самая редкая буква в русском языке – «Ъ».

Теперь я приведу примерный *алгоритм* , то есть последовательность шагов для расшифровки сообщения. Вот он:

1. Сначала надо точно подсчитать количество букв в сообщении. Для этого можно

взять чистый лист бумаги в клетку и для каждого символа шифрограммы откладывать одну незаполненную клеточку. Клеточки, соответствующие пробелам, надо подчёркивать. После того как всё сообщение будет переведено в клеточки, надо просто посчитать пустые клетки без подчёркиваний.

2. Дальше следует построить таблицу. В ней должно быть два столбца и столько строк, сколько разных символов используется в шифрограмме. В первый столбец надо вписать все использованные символы.

3. Затем необходимо подсчитать количество каждого из отдельных символов и записать результаты во второй столбец. Это самая занудная часть алгоритма, но сделать это необходимо. Может быть, это займёт у тебя очень много времени, поэтому приступай к подсчетам, только когда у тебя есть возможность и желание заниматься. Как только ты устанешь, надо отложить это занятие и заняться чем-нибудь другим. Так за несколько подходов ты сможешь довести дело до конца.

4. После того как частоты всех символов посчитаны, надо нарисовать ещё одну такую же таблицу. Однако теперь записывай в нее символы по убыванию частоты. В первой строке должен находиться самый часто встречаемый символ и его количество в тексте. Во второй строке – следующий по частоте и т. д. Ты уже понимаешь, к чему мы ведём?

5. Теперь организуй рабочий цикл. В шифрограмме ты видишь символ, который встречается чаще всего. А в русском языке чаще всего встречается буква «О». Можно выдвинуть *гипотезу* , то есть сделать предположение, что этот символ и есть буква «О». После этого впиши букву «О» в тот самый размеченный лист, с помощью которого мы считали буквы в сообщении – в те клетки, которые соответствуют самому часто встречающемуся символу.

6. Теперь посмотри на частично разгаданный текст. В нём могут встретиться слова, о значении которых можно догадаться. Например, если есть слово из двух букв, стоящее после запятой, и вторая буква в этом слове – «О», то наверняка это слово «НО». А уж если оно встречается несколько раз, и всегда после запятой, то это точно слово «НО». Значит, теперь у нас есть вторая буква – «Н». Но если таких предположений сделать нельзя, то надо вернуться к шагу 5 и предположить значение следующего неразгаданного и наиболее часто встречающегося символа.

7. К таблице, которую мы заполняли на шаге 4, необходимо пририсовать ещё один столбец. В него мы будем записывать расшифровки символов.

Так, повторяя шаги 5 и 6, ты сможешь расшифровать весь текст. Однако иногда предположения относительно соответствия символов могут оказаться неверными. Это часто происходит, когда разгаданных символов ещё не так много, чтобы уже можно было видеть целые слова, а частоты разгадываемых символов примерно одинаковы. Тогда надо делать шаг назад в рассуждениях и выносить иное предположение. Также возможно, что в шифрограмме намеренно снижены или повышены частоты некоторых букв, и это может ввести в заблуждение. Но грамотный криптоаналитик в конце концов расшифрует и такой текст.

Давай попробуем разгадать по этому алгоритму ту шифрограмму, которая приведена несколькими страницами раньше. А после этого ты сможешь самостоятельно сделать то же самое с любой другой шифрограммой, текст в которой зашифрован этим способом, но, возможно, при помощи других значков.

Итак, в шифрограмме 419 букв (если твой результат отличается на пару букв, это не страшно, поскольку такая неточность не повлияет на результаты. А вот если ты ошибёшься на десяток букв, то тут уже придётся пересчитывать).

Теперь начнём считать частоты символов. В результате должна получиться примерно такая таблица:

ტ	11
ხ	17
ფ	30
ყ	12
ვ	34
თ	44

Надеюсь, что ты заполнишь все остальные строки самостоятельно.

После того как таблица будет построена, строчки необходимо отсортировать по убыванию количества символов. Если это сделать, то в результате получится что-то вроде этого:

	45
	44
	34
	30
	27
	25

Как видно, здесь частота первых двух символов отличается только на единицу. Это очень неприятная ситуация, поскольку придётся делать гипотезы и проверять их. Впрочем, криптоаналитик при дешифровке всегда строит гипотезы и пытается их проверить. Так что давай сейчас построим одну гипотезу. Поскольку самой частой буквой в русском языке является «О», то предположим, что значок из первой строки отсортированной таблицы – это и есть буква «О». Что получится, если в соответствии с догадкой подставить эту букву в наш текст? Вот:

––––––. –––––––, ––О ––––––––––О–––––О––, –––––––––––––О––––––. ––––––О –––, –О ––О–––О––––––––––О–О–. –––––––––––––О–––––––, ––––––О––О––О––––––О–––––О–––––––––О –––О–––––––––––––––––––––––––––––––––О–. –О–––О––––––О–––––––––––О––––––––. ––, –––––О––О ––––––––О–––––––О––О––––––––––, ––О––––––О –––О––––––––––– (––О–––––, –О––––––О––––––––––О–––––––––). ––О ––––––––О–––О, –––––О –О–––––––––––––––––––––––––––––, ––О–О –––––––––––––––––––––––––––––О–––О––––––О.

Не очень-то понятно. Тем не менее это уже что-то.

Что делать дальше? Теперь попробуем подставить следующую по частоте букву. Для русского языка это буква «Е», так что подставим её вместо символа, занимающего вторую строчку в отсортированной таблице. Вот что получится после этого:

–––––Е. –––––––, –ЕО – Е–––––––––О––––––О––, – Е–––Е––––––ЕОЕ Е–––Е. –––––ЕО Е––, ЕО ––О–––О–––Е––– ЕО–О–. ––– Е– Е–––––––О––––––––, ––––––О–ЕО––О––Е––О–––––О––––––––––О –––О––Е––––––––––––––––– Е––––––––––ЕО–. –О–ЕО––––––О–––––––––––О––––––––. – Е–––––––––Е–––––––––––––Е––– Е–––––––––, –––––О––О ––––––––О––Е–––О––О––––––– Е––, –ЕО–––––––ЕО –––О–––––––––––Е– (––О––

Е−−, −О−− Е−−О−−−−−−−−−О−−−−−−Е−). −ЕО −− Е−−−−О−−О, Е−−−ЕО −О−−−−−−−−−−−−−−−− Е−−−−−−−−, −−О−О Е−−−−−−−−−−−−−Е−−−−−Е−−−−О−ЕО−Е−−−−О.

Сразу видно, что тут что-то не то. Во-первых, можно обратить внимание на слово «ЕО» в первой строке (шестнадцатое слово). Такого слова нет в русском языке. Во-вторых, в тексте неоднократно встречается не до конца разгаданное слово «−ЕО», причём на первом месте стоит один и тот же символ (это слово встречается четыре раза). Какие слова из трёх букв, подходящие под эту форму, есть в русском языке? Посмотрим: ГЕО (довольно редкое болгарское имя), ЛЕО (фамилия или имя из английского языка), НЕО (это из «Матрицы») и РЕО (город во Франции). Как видно, обычного русского слова нет ни одного, и можно предположить, что мы неверно расшифровали первые буквы. Впрочем, уже несуществующее слово «ЕО» позволяет отбросить гипотезу насчёт буквы «Е».

Теперь ты понимаешь, что «короткие» слова на первом этапе могут принести очень большую пользу. Именно на короткие слова надо обращать внимание, когда ты только приступаешь к расшифровке секретного сообщения. Давай пойдём дальше. Таким же образом можно отвергнуть гипотезы о том, что этот второй символ – буква «А» (третья по частоте) или буква «И» (четвёртая). Да, слова «АО» (сокращение от «автономный округ») и «ИО» (спутник Юпитера или имя нимфы из греческой мифологии) в русском языке есть, но они редкие и вряд ли окажутся в этом тексте.

Идём дальше. Следующая по частоте буква – это «Н». Тут, казалось бы, всё нормально, поскольку слово «НО» в русском языке есть, и оно как раз часто стоит после запятой. И буквосочетание «−НО» может означать часто встречающееся слово «ОНО» (но не в нашем случае, ты же понимаешь почему?). Попробуем сформулировать гипотезу и заменить символ буквой:

−−−−−Н. −−−−−−−, −НО − Н−−−−−−−О−−−−−О−−, − Н−−−Н−−−−−НОН Н−−−Н. −−−−−НО Н−−, НО −−О−−−О−−−Н−−− НО−О−. −−− Н− Н−−−−−−О−−−−−−−, −−−−−−О−НО−−О−−Н−−О−−−−О−−−−−−−−О −−−О−−Н−−−−−−−−−−−−−−− Н−−−−−−−−−НО−. −О−НО−−−−−О−−−−−−−−−О−−−−−−−. − Н−−−−−−−−Н−−−−−−−−−−−Н−− Н−−−−−−−, −−−−О−−О −−−−−−О−−Н−−−О−−О−−−−−− Н−−, −НО−−−−−НО −−−О−−−−−−−−−−Н− (−−О−− Н−−, −О−− Н−−О−−−−−−−−−О−−−−−−Н−). −НО −− Н−−−−О−−О, Н−−−НО −О−−−−−−−−−−−−−−−− Н−−−−−−−−, −−О−О Н−−−−−−−−−−−−−Н−−−−−Н−−−−О−НО−Н−−−−О.

Час от часу не легче. Но тут легко можно заметить одиннадцатое слово «−НОН», причём первой буквой у него стоит та же, что и в слове «−НО». В русском языке есть слово «ОНОН» (река в Сибири), но оно не подходит, поскольку букву «О» мы уже отгадали. То есть гипотеза о букве «Н» – некорректная. Попробуем следующую букву, и если она не подойдёт, то придется поставить под сомнение самую первую гипотезу о букве «О». Следующая по частоте буква – это буква «Т». Подставим:

−−−−−Т. −−−−−−−, −ТО − Т−−−−−−−О−−−−−О−−, − Т−−−Т−−−−−ТОТ Т−−−Т. −−−−−ТО Т−−, ТО −−О−−−О−−−Т−−− ТО−О−. −−− Т− Т−−−−−−О−−−−−−−, −−−−−−О−ТО−−О−−Т−−О−−−−О−−−−−−−−О −−−О−−Т−−−−−−−−−−−−−−− Т−−−−−−−−−ТО−. −О−ТО−−−−−О−−−−−−−−−О−−−−−−−. − Т−−−−−−−−Т−−−−−−−−−−−Т−− Т−−−−−−−, −−−−О−−О −−−−−−О−−Т−−−О−−О−−−−−− Т−−, −ТО−−−−−ТО −−−О−−−−−−−−−−Т− (−−О−− Т−−, −О−− Т−−О−−−−−−−−−О−−−−−−Т−). −ТО −− Т−−−−О−−О, Т−−−ТО −О−−−−−−−−−−−−−−−− Т−−−−−−−−, −−О−О Т−−−−−−−−−−−−−Т−−−−−Т−−−−О−ТО−Т−−−−О.

Вновь обратим внимание на слова «−ТО» и «−ТОТ», у которых первая буква

одинаковая. Тут вариант один: первая буква – это «Э». Попробуем подставить:

−−−−−−Т. −−−−−−−−, −ТО − Т−−−−−−−−−О−−−−−−О−−, − Т−−−Т−−−− ЭТОТ Т−−−Т. −−−− ЭТО Т−−, ТО −−О−−−О−−−Т−−− ТО−О−. −−− Т− Т−−−−−−−О−−−−−−−−, −−−−−−−О−ТО−−−О−−−Т−−О−−−−−О−−−−−−−−−О −−−О−−Т−−−−−−−−−−−−−−−−− Т−−−−−−−−−−−ТО−. −ОЭТО−−−−−−О−−−−−−−−−−О−−−−−−−−. − Т−−−−−−−−−−Т−−−−−−−−−−−−−Т−− Т−−−−−−−−−, −−−−−О−−О −−−−−−−О−−Т−−−−О−−О−−−−−−− Т−−, −ТО−−−−−−ТО −−−О−−−−−−−−−−−Т− (−−О−− Т−−, −О−− Т−−О−−−−−−−−−−О−−−−−−−−Т−). ЭТО −− Т−−−−О−−О, Т−−−ТО −О−−−−−−−−−−−−−−−−−− Т−−−−−−−−−−, −−О−О Т−−−−−−−−−−−−−−−−Т−−−−−−Т−−−−−О−ТО−Т−−−−−О.

Пока всё нормально. Никаких противоречий на первый взгляд нет. Более того: в тексте встречается последовательность «−ОЭТО−−». В этом слове из семи букв открыты четыре, так что можно попробовать догадаться, какое это слово. Поиск по словарю даёт только одно слово: «ПОЭТОМУ». Более того, перед «ПОЭТОМУ» часто пишется запятая, как и в этом случае. Получается, что мы сейчас смогли выдвинуть вполне правдоподобную гипотезу относительно ещё трёх скрытых символов. Пора составить новую таблицу и заполнить её:

	45	О
	44	Т
. . .		
	11	М
	11	П
. . .		
	9	У
. . .		
	4	Э

Подставим-ка все известные на текущий момент символы в шифрограмму. Вот что

получится:

П−−−−Т. −−−−−−−, −ТО У Т−−−−−− ПО−У−−−О−−, − Т−−−Т−−−− ЭТОТ Т−−−Т. −−−− ЭТО Т−−, ТО − МО−У −О−−−Т−−− ТО−О−. −−− Т− Т−П−−− ПО−−М−−−−, −−−− П−О−ТО− ПО−−Т−−О−−−−О−−−−−−−−О −−−О−−Т−−−−−−−−−−−−−−− Т−−−−−−−−−ТО−. ПОЭТОМУ −−−О−−−−М −− ПО−−−У−−−. − Т−−−−−−−−Т−−−−−−−−−−−Т−− Т− У−−−−−−, −−− МО−−О −−−−−−О−−Т−−−О− ПО−−−−−− Т−−, −ТО−−−−−ТО −− МО−−−−−−−−−Т− (−−ОМ− Т−−, −ОМУ Т−−О−−−−−−−−−О−−−−−−Т−). ЭТО −− Т−−−−О−−О, Т−−−ТО −О−−−−−−−−−П−−−−− Т−−П−−−−М, −−О−О Т−−−−−У−−−−−−−−Т−− УМ−Т−−−МО−ТО−Т−−−−О.

Сразу бросается в глаза первое слово. Ты ещё не догадываешься, что это за слово такое? Тогда подумай, какое слово из шести букв обычно ставят в начале письма, причём начинается оно на «П», а заканчивается на «Т»: «П−−−−Т». Ну, конечно же, это слово «ПРИВЕТ». Ура, у нас есть ещё четыре буквы. Давай внесём их в таблицу расшифровок:

ა	45	О
თ	44	Т
ე	34	Е
ფ	30	И
. . .		
ზ	17	Р
. . .		
ც	12	В
. . .		
ლ	11	М
ր	11	П
. . .		
ჯ	9	У
. . .		
ვ	4	Э

Вот, что получается, если теперь подставить все эти буквы в шифрограмму:

ПРИВЕТ. −−−Е−−−, −ТО У ТЕ−− В−− ПО−У−И−О−−, И Т−−ИТ−Е−− ЭТОТ ТЕ−−Т. Е−−И ЭТО Т−−, ТО − МО−У −ОР−ИТ−−− ТО−О−. −−− Т− ТЕПЕР− ПО−ИМ−Е−−, −И−Р

ПРО−ТО− ПО−−Т−−ОВ−И −ОВЕР−Е−−О −Е −О−ИТ−−−−−−−Р−В−−И− Т−−− И −Е−РЕТОВ. ПОЭТОМУ −И−О−−− ИМ −Е ПО−−−У−−−. В ТЕ−Е−ИЕ −ЕТ− И −−−И−−−−−ТИ− Т−У−−−Е−−, −−− МО−−О −−−И−РОВ−Т−−ВОИ ПО−−−−И− Т−−, −ТО−−−И−ТО −Е МО− И−Р−−−Р−Т− (−РОМЕ ТЕ−, −ОМУ Т−−ОВЕРИ−−−ВОИ −Е−РЕТ−). ЭТО −Е Т−−−−О−−О, Т−−−ТО −О−ЕРИ−− И −−П−−И−− ТЕРПЕ−ИЕМ, −−ОРО Т− В−−−У−Е−−−−−Т− И УМЕТ−−−МО−ТО−ТЕ−−−О.

Что же, неплохо. Тут уже видно несколько слов, кроме тех, которые мы разгадали. Самые очевидные из них – «ТЕПЕР−» (даёт «Ь»), «−РОМЕ» (даёт «К») и «ТЕРПЕ−ИЕМ» (даёт «Н»). Подставим новые буквы в шифрограмму и получим:

ПРИВЕТ. Н−−Е−−Ь, −ТО У ТЕ−− В−− ПО−У−И−О−Ь, И Т−−ИТ−Е−Ь ЭТОТ ТЕК−Т. Е−−И ЭТО Т−К, ТО − МО−У −ОР−ИТЬ−− ТО−О−. К−К Т− ТЕПЕРЬ ПОНИМ−Е−Ь, −И−Р ПРО−ТО− ПО−−Т−НОВКИ −ОВЕР−ЕННО НЕ −О−ИТ−−−−−−КР−В−НИ− Т−−Н И −ЕКРЕТОВ. ПОЭТОМУ НИКО−−− ИМ НЕ ПО−Ь−У−−−. В ТЕ−ЕНИЕ −ЕТ− И Н−−И−−−Н−ТИ− Т− У−Н−Е−Ь, К−К МО−НО −−−И−РОВ−ТЬ −ВОИ ПО−−−НИ− Т−К, −ТО−− НИКТО НЕ МО− И− Р−−КР−ТЬ (КРОМЕ ТЕ−, КОМУ Т−−ОВЕРИ−Ь −ВОИ −ЕКРЕТ−). ЭТО НЕ Т−К −−О−НО, Т−К −ТО −О−ЕРИ−Ь И −−П−−И−Ь ТЕРПЕНИЕМ, −КОРО Т− В−−−У−Е−Ь −Н−ТЬ И УМЕТЬ −−МО−ТО−ТЕ−ЬНО.

Собственно, дальше ты сможешь всё доделать самостоятельно. Сообщение стало настолько прозрачным, что ни одна буква больше не утаится. Доделай то, что мы начали, до конца, и ты сможешь прочитать это тайное послание.

Это упражнение должно было научить тебя нескольким полезным вещам, а именно:

1. Применять методы расшифровки, основанные на частотном анализе и подборе ключевых слов. Это прямой навык, который мы изучили на этой неделе.

2. Теперь ты понимаешь, что в скрываемых текстах нельзя использовать слова, о которых можно догадаться. Если ты начинаешь зашифрованное письмо со слова «привет» или «здравствуйте», то считай, что никакого секрета больше нет. В шифрограммах ни в коем случае нельзя употреблять слова, о которых в первую очередь подумает криптоаналитик. Всегда ставь себя на место того, кто попытается разгадать твой код, и думай, какие слова ты бы проверил в первую очередь. Избегай этих слов.

3. Шифрограммы должны быть достаточно короткими, чтобы к ним нельзя было применить описанный метод анализа. Если ты зашифруешь одним шифром повесть на тысячу слов, то будь уверен, что этот секрет разгадают сразу же. А текст из десятка слов разгадать будет довольно сложно.

4. Наконец, в шифрограммах нежелательно употреблять короткие слова: предлоги, союзы, частицы, встречающиеся в обычных текстах много раз. Это всё – первые подсказки для криптоаналитика, при помощи которых он сможет взломать шифр. Сообщение вполне может быть понятным без предлогов и частиц: «Прибыть пункт распределения завтра десять тридцать». Попробуй зашифровать эту фразу каким-нибудь шифром простой подстановки, а потом применить к ней метод частотного анализа, и ты увидишь, насколько это сложнее.

На этом всё. Надеюсь, что тебе понравился наш первый урок. На следующей неделе мы изучим кое-что более сложное.

Неделя 2. Шифр многоалфавитной замены

Перед тем, как мы начнём изучать новый, более секретный способ шифрования и расшифровки (если помнишь, прошлый способ в принципе несекретен), я хотел бы договориться с тобой о паре важных вещей.

Во-первых, давай считать пробел символом. Да, с математической точки зрения пробел – это такой же символ, как и любой другой. Я специально использую слово «символ», а не

«буква», чтобы не путать. Итак, все буквы, цифры, пунктуационные знаки и даже пробел являются *символами* . Но главное – это понять, что пробел – не отсутствие символа, а отдельный символ. В предложении «ЭТА ФРАЗА СОДЕРЖИТ 3 °СИМВОЛОВ» действительно содержится 30 символов: 24 буквы, 2 цифры и 4 пробела.

Во-вторых, давай в дальнейшем для шифрования использовать только заглавные буквы русского алфавита и пробел, причём будем считать пары букв «Е» и «Ё», а также «Ъ» и «Ь» неразличимыми. Теперь в наших текстах и шифрограммах символ «Е» будет обозначать как букву «Е», так и букву «Ё», а символ «Ъ» будет обозначать буквы «Ъ» «Ь». Таким образом, весь алфавит теперь состоит из следующих символов:

Пробел А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я

Примечательность этого алфавита в том, что в нём содержится *ровно* 32 символа.

С каждым из этих символов мы сопоставим число от 0 до 31, которое назовём *кодом* . То есть «пробел» будет иметь код 0, буква «А» – код 1 и так далее – до буквы «Я», которой мы присвоим код 31.

После этого надо научиться складывать и вычитать особым образом (математики называют такие операции сложением и вычитанием с вычетами). Итак, у нас есть только тридцать два числа – от 0 до 31. Мы хотим складывать и вычитать при помощи этих чисел, и никакие другие числа нам использовать нельзя. Очень просто, например, сложить 5 и 8, поскольку получится 13. Но как быть, если нам надо сложить, скажем, 23 и 17? Обычная арифметика подсказывает, что 23 + 17 = 40, но у нас нет чисел, которые больше 31. Как быть? Всё просто. Если полученный результат больше 31, надо вычесть из него общее количество чисел, то есть 32. Другими словами, по правилам нашей новой арифметики (немного странной на первый взгляд) получается, что 23 + 17 = 40–32 = 8.

То же самое с вычитанием. Легко вычесть из 15, скажем, 12, поскольку получится 3. А как вычесть из меньшего числа большее, например, из 10–27? Тут тоже просто. Если из меньшего числа требуется вычесть большее, то сначала к меньшему надо прибавить 32. Таким образом: 10–27 = 10 + 32–27 = 15.

Такие правила называются *арифметикой остатков* или *вычетов* . Криптографы постоянно работают с этими не совсем обычными для нас арифметическими правилами. Но для криптографии они очень даже обычны.

Мы узнали об этой новой арифметике для того, чтобы использовать её правило сложения для шифрования, а правило вычитания – для расшифровки. Ведь у каждой буквы есть числовой код от 0 до 31. При таком шифровании буквы открытого текста складываются со специально выбранными буквами (эти выбранные буквы называются «*ключом* » или «*паролем* »). Расшифровывают сообщение, вычитая из букв зашифрованного текста буквы ключа.

Если в качестве ключа взять какую-нибудь одну букву, то получится шифр одноалфавитной замены, который мы как раз изучали на прошлой неделе.

Давай попробуем зашифровать слово «БЕСПОРЯДОК» при помощи ключа «С». Начнём с первой буквы, «Б». Её код – 2, а код буквы «С» – 18. Если сложить буквы Б и С, то есть 2 и 18, то получится 20, а это буква «У». Далее, буква «Е», её код – 6. Опять складываем: 6 + 18 = 24, и это буква Ч. Продолжая так дальше, мы получаем слово «УЧГБАВРХАЭ». Расшифровывать это слово нужно при помощи вычитания. Берём букву «У» и её код 20, вычитаем из него код буквы «С»: 20–18 = 2, и получается буква «Б». Ну и так далее…

Итак, теперь мы знаем, какие математические правила используются для шифрования при помощи одноалфавитной замены. Тогда что же такое многоалфавитная замена? При одноалфавитной замене каждая буква открытого текста складывается с одной и той же буквой ключа. А при многоалфавитной замене символы ключа циклически изменяются. Это значит, что первая буква открытого текста шифруется первой буквой ключа, вторая буква – второй буквой, третья – третьей и так далее до, например, шестой буквы, которая снова шифруется первой буквой ключа, и цикл повторяется.

Как же выбираются эти буквы для шифрования? Как я уже сказал, для этого используется ключевое слово, ключ или пароль. Его длина определяет длину *цикла многоалфавитной замены* , то есть количество используемых алфавитов. А буквы ключа применяются для шифрования при помощи описанных выше правил арифметики вычетов. Давай рассмотрим пример. Пусть в качестве ключа используется слово «КЛЮЧ», тогда первая буква открытого текста шифруется через букву «К», вторая – через букву «Л» и так далее, а пятая буква открытого текста опять шифруется при помощи буквы «К».

Например:

П	К	Ъ
Р	Л	Э
И	Ю	Ж
Х	Ч	Н
О	К	Щ
Д	Л	Р
И	Ю	Ж
	Ч	Ч
З	К	Т
А	Л	М
В	Ю	А
Т	Ч	К
Р	К	Ы
А	Л	М
	Ю	Ю
К	Ч	В
	К	К
П	Л	Ы
Р	Ю	М
У	Ч	Л
Д	К	П
У	Л	

Вот и получился зашифрованный текст:

«ЪЭЖНЩРЖЧТМАКЫМЮВКЫМЛП».

Уверен, что его не сможет разгадать никто из твоих друзей. Никто даже и браться за такое не будет.

Есть и более легкий метод шифрования этим способом. Для него требуется одна

таблица. Она на следующем развороте.

Пользоваться ею легко. Для шифрования надо найти букву открытого текста в первой строке и букву ключа в первом столбце. Буква шифрограммы находится на пересечении выбранного столбца и строки. Для расшифровки надо найти букву ключа в первом столбце и букву шифрограммы в выбранной строке. Буква открытого текста будет в первой строке полученного столбца. Всё довольно просто.

Однако я рекомендую научиться использовать арифметику вычетов. В дальнейшем это очень пригодится. Это как с таблицей умножения: можно вызубрить её в том виде, в каком она приводится на тетрадных обложках. А можно понять правила умножения, и тогда без проблем перемножать любые числа.

Теперь давай научимся расшифровывать тексты, записанные шифрами многоалфавитной замены. Например, у тебя оказалось зашифрованное послание и ты знаешь, что оно зашифровано именно таким шифром. Как подступиться к расшифровке? Вот простейший метод:

1. Определить длину ключа, то есть длину цикла, в котором меняются алфавиты. Это делается при помощи одного очень хитроумного способа, о котором ты узнаешь чуть позже.

2. Как только длина ключа установлена, у нас появляется столько шифрограмм (зашифрованных шифром одноалфавитной замены), из скольких символов состоит ключ. А взламывать такие шифрограммы ты уже умеешь, то есть твоя задача сводится к тому, что мы изучили на прошлой неделе. Да, в этот раз расшифровка намного более трудоёмкая, поскольку придется несколько раз подсчитывать частоты и выдвигать гипотезы, а это непросто. Кроме того, надо суметь не запутаться и сопоставить расшифровки друг с другом. Но при должном умении и старании все получится.

Чтобы узнать длину ключа, используются два метода. Один из них очень трудоёмкий и требует множества вычислений (в наше время их можно поручить компьютеру, а раньше ими обычно занималась целая комната специально обученных сотрудников со счётами или счётными машинками). Но этот метод гарантированно определяет длину ключа. Ты можешь прочитать о нем в специальной литературе или справочниках – он называется «*метод индекса совпадений* ».

		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
А	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Б	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
В	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Г	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э
Д	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю
Е	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я
Ж	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	
З	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А
И	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б
Й	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В
К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г
Л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д
М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е
Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж
О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И
Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й
С	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К
Т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
У	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
Ф	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
Х	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Ц	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Ч	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Ш	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
Щ	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ъ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Ы	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Э	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ю	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Я	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч

А вот второй метод – именно что хитроумный, но не всегда работает. Его мы и изучим. Он называется «метод Фридриха Касиски[1]». Идея заключается в том, что в обычном языке, на котором говорят люди, очень часто повторяются некоторые группы символов. Это коротенькие словечки или даже буквосочетания вроде многочисленных «ОРО» и «ОЛО» в русском языке. Грамотный шифровальщик избегает использования коротких словечек (об этом мы уже рассуждали на прошлой неделе), но вот с частыми буквосочетаниями это сделать сложно. Так что надо искать в шифрограмме такие повторяющиеся буквосочетания.

Итак, в шифрограмме мы ищем повторяющиеся группы символов. Лучше всего, чтобы длина этих групп была не менее трёх символов: если будет меньше, то велик шанс пойти по ложному следу. Это происходит из-за того, что разные двухбуквенные сочетания из

[1] **Фридрих Вильгельм Касиски –** Немецкий криптограф и археолог. В 1863 году опубликовал труд «Тайнопись и искусство дешифрования», в котором детально описал методы расшифровки текстов, зашифрованных шифрами многоалфавитной замены. При помощи этих методов был взломан шифр, который считался неприступным более четырехсот лет.

шифруемого текста были зашифрованы при помощи разных символов в ключе, а в результате получились одинаковые буквосочетания в шифрограмме. Если группа символов длиннее, то такого практически не происходит.

Расстояния между последовательными появлениями одинаковых групп в шифрограмме будут кратны длине ключа. Так что мы подсчитаем расстояния между всеми этими группами, а длина ключа будет равна наибольшему общему делителю всех расстояний.

Иногда это не срабатывает, так как из-за использования большого числа алфавитов разные группы символов исходного текста могут случайно получиться одинаковой группой в шифрограмме. Такое возможно, если текст очень большой. Тогда криптоаналитик должен внимательно изучить разные возможности и отсеять то, что не подходит. Мы не будем практиковаться в этом занятии, но я должен сказать о том, что такая возможность есть.

После того как длина ключа определена, вся шифрограмма выписывается в колонку. Ее ширина равна количеству символов в ключе. Затем надо сделать частотный анализ (который мы изучили на первой неделе) для каждого столбика этой колонки.

Давай потренируемся во всем этом на практике. Представь себе, что ты видишь такое послание:

ТИЪРУЫМТУНРШАТПЮАКЧЧЙАЙТГЗУШМНОЧЖАЧЗСЦСЮЙЗЗЫХШЮХАФЭБ
ДЦПЯХИСЫУХЮЭАППЖХКТУИЩЩЖЗЭШУЗЭЫШНТБАЩЪБЗХЮЦПЗЭШПЙДБЕРЫ
БАЧ
БТЪЮТПФАЫЗБМБЪФЯЫХЮТГЩФТСИАДШРБОГИБНАККВПУЭСУВООЦТБАИЫХФ
ФЕЙФДДРДТПЧФГБЯЧЭАРОФЭЪЙТЛШПЭМНОХОРЫУУНЪНОГЫТРЦЛЕПФВТЛИЩТ
ЙЗСТРШЮЛМГШТСИЦТ
ЗДБШЫОЪБЖСЫУВОБАЧЮЯОЦШТВНАВПУФЪОЦАЕЙЗБУЛРДТЩРГГПКОЮБТЮЭА
ЙКТОРОФЭУПТЕУЧАБЗЩЯЯПТЩРГГПЛ
ТНФПТГЗЩБОНЖАПФПЫУЦТШАЙВЧЖЪОХИУЮБХПТУНЫТЛЦЫЖАРЭЕЖШФДОЦ
ОШЖЗАБЕНЩЙФЮШАХЮТВУПЦПМПГЗЛЕПФВТФЧУЗХФАЙЕОЕЭЗВЩЖЗЫБЗНЗНА
ЧЮА
ЪЙТЙЗЯБЕЫЫУУВОАБЗБШНЫОЮБТОПОЭБАРЦЖХЧЕЫЗЛЕПЪОДРЦАБВЗЗЫХШЮХ
БХЧСАББВГОБОЗАЕБУОУВЩЮЯЯЪЭБАХФХИУПЭКПШНГЫТЕНЪБС

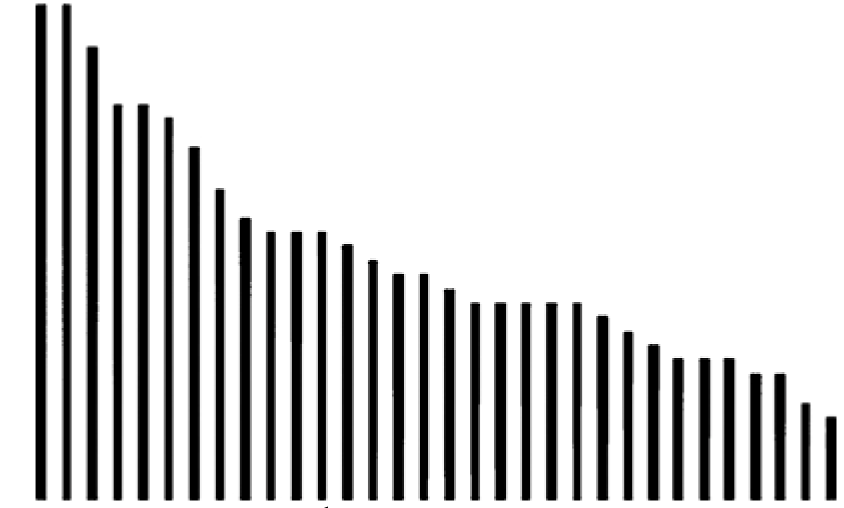
Если сделать здесь частотный анализ, то получится вот такая таблица:

Символ	Количество	Частота		Буква	Частота
Б	35	6,27%		О	11,80%
Т	35	6,27%		Е, Ё	8,41%
А	32	5,73%		А	7,92%
О	28	5,02%		И	6,83%
П	28	5,02%		Н	6,72%
З	27	4,84%		Т	6,18%
У	25	4,48%		С	5,33%
Ы	22	3,94%		Л	5,00%
Ф	20	3,58%		Р	4,45%
ПРОБЕЛ	19	3,41%		В	4,33%
Х	19	3,41%		К	3,36%
Ш	19	3,41%		М	3,26%
Ю	18	3,23%		Д	3,05%

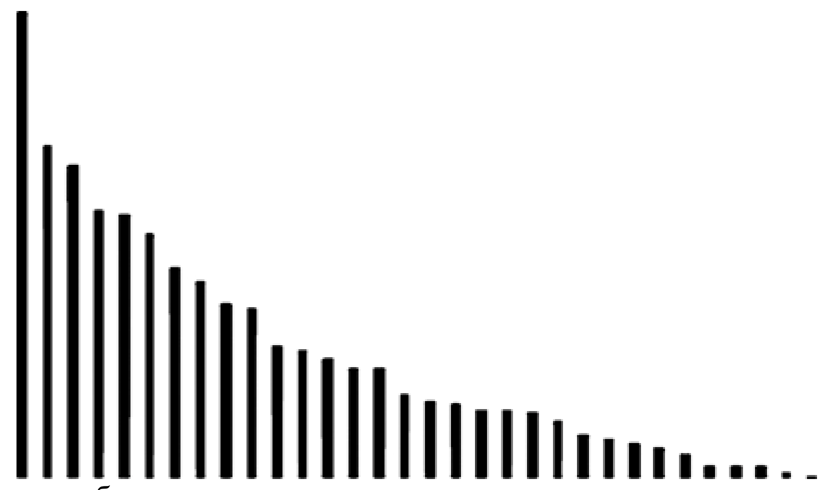
Н	17	3,05%		П	2,81%
Р	16	2,87%		У	2,80%
Э	16	2,87%		Я	2,13%
Е	15	2,69%		Ы	1,96%
В	14	2,51%		Ь	1,92%
Г	14	2,51%		З	1,75%
Й	14	2,51%		Г	1,74%
Ц	14	2,51%		Б	1,71%
Ч	14	2,51%		Ч	1,47%
Ъ	13	2,33%		Й	1,12%
Щ	12	2,15%		Ж	1,05%
Ж	11	1,97%		Х	0,89%
Д	10	1,79%		Ш	0,81%
И	10	1,79%		Ю	0,61%
С	10	1,79%		Э	0,38%
Л	9	1,61%		Щ	0,37%
Я	9	1,61%		Ц	0,36%
К	7	1,25%		Ф	0,19%
М	6	1,08%		Ъ	0,02%

Для удобства в двух крайних правых столбцах этой таблицы я привел частоты букв в русском языке. Уже беглый взгляд на эту таблицу подсказывает, что тут есть проблема. Частоты совершенно не совпадают, хотя длина шифрограммы значительная (558 символов).

Что делают настоящие криптоаналитики для анализа подобной ситуации? Они строят графики. Вот два графика (они называются «гистограммами»):



Гистограмма частот символов в шифрограмме


Гистограмма частот букв русского языка

Ты можешь представить себе, что эти графики – набор вертикальных штырьков, на которые нанизаны блины, как в детской пирамидке или головоломке «ханойская башня». Количество блинов на штырьке соответствует количеству целых процентов, а последний блин по толщине соответствует долям процента. Если расположить эти башни по убыванию количества блинов, то как раз получатся такие гистограммы. По горизонтали отложены буквы по убыванию частот их в языке, а по вертикали – относительные частоты в процентах.

Видишь, на этих графиках обозначены подсчитанные частоты символов. На левом графике отложены частоты символов из шифрограммы, а на правом – частоты букв русского языка. Вид графиков различается: для шифрограммы он более пологий. Это уже указывает на то, что нарушено распределение частот, а значит, для шифрования был избран не одноалфавитный шифр, а что-то другое. Кстати, в качестве тренировки рекомендую построить такую гистограмму для символов из шифровки первой недели: ты увидишь, что она очень похожа на гистограмму частот для букв русского языка.

Итак, мы с помощью математических методов убедились, что это не одноалфавитная замена. Возможно, это многоалфавитный шифр. Попробуем проверить. Как я уже сказал, следует сначала попытаться найти длину ключа. Для этого в шифрограмме надо искать одинаковые последовательности букв. Это сложно, и надо собрать всё своё внимание, чтобы найти их.

Быстрый просмотр шифрограммы показывает, что есть одно семисимвольное сочетание «ЗЗЫХШЮХ», которое встречается в шифрограмме дважды. При этом повторяющихся восьмисимвольных сочетаний нет. (Надо отметить, что чем больше в повторяющихся сочетаниях символов, тем лучше). Проверим, на каких позициях стоят эти буквосочетания. Первое стоит на позиции 49, а второе – на 509. Разница: 509 – 49 = 460. Запомним.

Больше семисимвольных сочетаний нет, поэтому посмотрим на шестисимвольные. Есть четыре таких буквосочетания, но первые два из них – это префикс и суффикс семисимвольного сочетания, рассмотренного ранее, поэтому учитывать их не будем. Другие – это «ЛЕПФВТ» и «ТЩРГГП». Первое из этих двух буквосочетаний встречается на позициях 225 и 421. Их разница: 421–225 = 196. Второе стоит на позициях 294 и 330, и разница составляет 330–294 = 36.

Итак, у нас есть три числа, три разницы: 460, 196 и 36. Рассмотрим наибольший общий делитель этих чисел. Он равен 4. В принципе, на этом можно остановиться, поскольку мы только что нашли длину ключа. Теоретически, ключ может быть длиной в 2 символа (поскольку 4 делится на 2), но можно предположить, что никто не будет кодировать сообщение при помощи такого короткого ключа. Если бы у нас в качестве наибольшего общего делителя получилось число 8, то нам пришлось бы проверить ещё и пятисимвольные сочетания, а потом и все остальные, чтобы убедиться, что длина ключа равна именно 8, а не

4.

Итак, мы определили длину ключа и теперь можем выписать всю шифрограмму в четыре колонки, для каждой из которых применить уже известный нам частотный анализ. Вот как это будет выглядеть:

ТИЪР
УЫМТ
УНРШ
АТПЮ
АКЧЧ
ЙАЙТ
ГЗУШ
МНОЧ
ЖАЧЗ
СЦСЮ
ЙЗЗЫ
ХШЮХ
АФЭБ
ДЦПЯ
…

Но есть метод быстрее и проще. Он не даёт гарантии мгновенного нахождения ключа, но, по крайней мере, не надо заниматься длительным подсчётом частот. Вернее, подсчитать кое-что надо, но это намного быстрее и менее утомительно. В общем, как обычно это бывает у криптоаналитиков, надо не кидаться с головой в скучные подсчёты (они помогут, но сильно надоедят), а сесть и подумать. Решение придёт.

Итак, мы разобрались с длиной ключа и распределили буквы шифрограммы по столбцам (то есть по алфавитам). Теперь они полностью соответствуют частотам употребления букв (и пробела) в русском языке. Поскольку пробел встречается чуть ли не в два раза чаще, чем самая частая буква русского алфавита «О», то резонно предположить, что самый частый символ в каждом столбце обозначает пробел.

А теперь, если ты внимательно изучишь таблицу, приведённую ранее, то увидишь, что у пробела – код 0. Это значит, что при сложении с ним символ не меняется. Получается, что самая часто встречающаяся буква в каждом столбце и есть буква ключа. Вот это да!

Давай подсчитаем. Вот первый столбец:

«ТУУААЙГМЖСЙХАДХУАЖУЖУШАЗППЕАТПЫБЫГСШГАПУОАХЙДПБАЭЛМ ОУОРПЛЙРМСШБУАОВПОЙЛЩПБАОЭЕБЯЩПНГОПУАЖИБУЛАЖОЖЕЙАВППФЗЙЭ ЖЗА ЙЕУБНБПАЖЫПРВХБАВОБВЯАИЭНЕБ».

Можно заметить, что чаще всего здесь встречается буква «А». Итак, первая буква ключа найдена. Я рекомендую тебе тщательно подсчитать в каждом столбце количество букв и определить наиболее часто встречающуюся, после чего понять ключ.

Если у тебя все получилось, то нашелся ключ – «АЗОТ» (это газ). И теперь можно легко расшифровать секретное послание. Как я уже писал, надо из шифрограммы вычесть ключ по модулю 32. Вот так:

ТИЪР		АЗОТ		САЛЮ
УЫМТ		АЗОТ		ТУЮ
УНРШ		АЗОТ		ТЕБЕ
АТПЮ		АЗОТ		КАК
АКЧЧ		АЗОТ		ВИДИ
ЙАЙТ		АЗОТ		ШЬ В
ГЗУШ		АЗОТ		ДЕЛ
МНОЧ	–	АЗОТ	=	Е ДЕ
ЖАЧЗ		АЗОТ		ШИФР
СЦСЮ		АЗОТ		ОВКИ
ЙЗЗЫ		АЗОТ		ШИФ
ХШЮХ		АЗОТ		РОВ
АФЭБ		АЗОТ		МНОГ
ДЦПЯ		АЗОТ		ОАЛФ
…		…		…

Если всё сделано правильно, то проявится открытое сообщение: «САЛЮТУЮ ТЕБЕ. КАК ВИДИШЬ, В ДЕЛЕ ДЕШИФРОВКИ ШИФРОВ МНОГОАЛФАВИТНОЙ ЗАМЕНЫ ТАКЖЕ НЕТ НИЧЕГО СЛОЖНОГО. НЕОБХОДИМО ПРОСТО ОЧЕНЬ ТЩАТЕЛЬНО ВСЁ РАССЧИТЫВАТЬ, ВЫПОЛНЯТЬ МНОГО АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ И БЫТЬ КРАЙНЕ ВНИМАТЕЛЬНЫМ. ПОЭТОМУ, КАК И В ПРОШЛЫЙ РАЗ, Я ХОЧУ ЗАЯВИТЬ О ПОЛНОЙ БЕСПОЛЕЗНОСТИ ТАКИХ ШИФРОВ. КАКОЙ БЫ НИ БЫЛА ДЛИНА КЛЮЧА, ШИФРОГРАММА В КОНЕЧНОМ ИТОГЕ БУДЕТ ВЗЛОМАНА ТЕМ, КОМУ ИНТЕРЕСНО ЕЁ СОДЕРЖИМОЕ. НО БЛАГОДАРЯ ЭТОМУ УПРАЖНЕНИЮ ТЫ УЖЕ МОЖЕШЬ ПОНЯТЬ И ПОДУМАТЬ НА ТЕМУ, КАК МОЖНО ИЗМЕНИТЬ ЭТОТ СПОСОБ ШИФРОВАНИЯ, ЧТОБЫ ОН СТАЛ АБСОЛЮТНО НЕВЗЛАМЫВАЕМЫМ. ДЕРЗАЙ».

Что ж, ещё пара моментов:

1. Не всегда пробел будет самым частым символом в столбце. Если не удалось обнаружить ключ, то можно попробовать либо вычитать букву «О», либо попытаться использовать в качестве пробела второй по частоте символ. Ключ часто может быть каким-то словом.

2. Но по-настоящему хитрые шифровальщики никогда не делают ключом слово. Если из самых часто встречаемых символов в каждом столбце получилось не слово, а какое-то бессмысленное буквосочетание, то попробуй все же применить его в качестве ключа. Вполне может быть, что это и есть ключ (всё-таки пробел очень часто встречается).

Теперь ты можешь обдумать и такую проблему: как можно модифицировать этот способ шифрования, чтобы его было не так легко взломать (а это тоже был достаточно лёгкий взлом)? Поразмышляй насчёт длины ключа.

Надеюсь, что на этой неделе тебе понравилось разгадывать зашифрованные сообщения, несмотря на множество вычислений. Ведь по сравнению с тем, чем мы занимались на первой неделе, это был настоящий шифр. А уж на следующей неделе тебя ждёт нечто удивительное. Уверен, что такого тебе ещё не попадалось.

Неделя 3. Стеганография и код Фрэнсиса Бэкона

Представь, что ты получаешь вот такое письмо:

*При**в** ет **теб** е, мой **д** ор**ог** ой с**ы** н. К**а** к п**ож** ив**а ешь** в **де** ревне? Чт**о** новог**о** слы**ш** н**о** ? **Р** уг**ае** шь**с** я **л** и **с де** д**у** шкой и баб**ушко** й**? У н** ас с ма**м** ой всё к**а** к о**б** ы**чно** . Х**одим н** а рабо**ту** . Приед**е** м **к те** бе н**а с** л**е** ду**ющих вых одны** х, **г ото** вься. Кушай хорошо, не балуйся и слушайся старших. Ешь больше овощей и фруктов, поменьше играй на планшете и побольше гуляй. Катайся на велосипеде и купайся. До скорой встречи, твой отец.*

И больше ничего. Никаких шифровок, ничего такого, о чём мы говорили раньше. Это странно.

А теперь посмотри на этот текст внимательнее. Почему в нём использованы обычные и жирные буквы? Обычно так никто не пишет. Нет ли тут какой-то тайны, над которой надо бы поломать голову?

Действительно, ты уже можешь догадаться, что в этой книге ничего не написано просто так. Тут явно что-то закодировано. Но для того чтобы это понять, необходимо немного отвлечься и изучить новую для тебя тему из математики. Тут уж ничего не поделаешь, поскольку криптография – это наука, в которой очень много математики. И даже если тебе математика не очень нравится, то я надеюсь, что ты её полюбишь, прочитав до конца эту книгу и вместе со мной попробовав все способы шифрования и расшифровки. Ведь математика позволяет решать такие интересные загадки! Честно говоря, математика позволяет делать практически всё, что только можно придумать.

Почему мы вообще используем счёт до десяти? Почему у нас десять цифр: 0 1 2 3 4 5 6 7 8 9? Почему, если прибавить к девяти единицу, то произойдёт так называемый *перенос разряда* и число станет двузначным? Для записи числа «десять» мы не вводим одиннадцатую цифру, а используем те же самые цифры, что и для первых десяти чисел от нуля до девяти. А что вообще обозначает запись «10»? Эта запись обозначает: один десяток и ноль единиц. А, к примеру, запись «156» обозначает: одна сотня, пять десятков и шесть единиц. А вот запись «7325» обозначает: семь тысяч, три сотни, два десятка и пять единиц.

А что, если бы у нас было не две руки и десять пальцев, а этакие щупальца, как у осьминога? Мы могли бы считать только до двух, и перенос разряда происходил бы, когда мы досчитывали бы не до десяти, а до двух. Это очень сложно воспринять при первом чтении, но ты постарайся: для записи любого числа можно обойтись всего лишь двумя цифрами: 0 и 1. Такова *двоичная система счисления* , и её постоянно используют программисты, а еще очень любят использовать математики, особенно криптографы.

Смотри: у нас есть всего две цифры, но мы хотели бы считать любое количество предметов, которое нам может встретиться. Когда предметов нет, мы используем цифру 0. Если предмет один, то мы используем цифру 1. А когда предмета два? Тут происходит перенос разряда, который в двоичной системе используется всегда, когда надо сложить 1 и 1. Так вот если надо посчитать два предмета, то мы запишем это так: 10. А три предмета? Это проще: 10 + 1 = 11. Если у нас четыре предмета, то надо к трём прибавить один, то есть 11 + 1. Что получится? Сложение делается точно так же, как и в десятичной системе. Сначала складываем единицы, получается 10, то есть происходит перенос разряда. Но в следующем разряде уже стоит 1, поэтому опять надо сложить единицы, и опять произойдет перенос разряда. Получается, что четыре предмета обозначаются как 100.

Вот так начинается счёт в этой замечательной системе счисления:

Ноль	0
Один	1
Два	10
Три	11
Четыре	100
Пять	101
Шесть	110
Семь	111
Восемь	1000
Девять	1001

Десять	1010
Одиннадцать	1011
Двенадцать	1100
Тринадцать	1101
Четырнадцать	1110
Пятнадцать	1111

Ты сможешь определить, как в двоичной системе обозначается шестнадцать предметов?

Как перевести такие двоичные числа в привычный вид? Тут надо сделать то же самое, что и в десятичной системе, только роль разрядов – единиц, десятков, сотен, тысяч и т. д. играют единицы, двойки, четвёрки, восьмёрки. Всё это – так называемые *степени основания системы счисления* (основание двоичной системы счисления – двойка). Если в системе счисления десять цифр, то перенос разряда происходит на десятках, а когда у нас только две цифры, то приходится делать перенос разряда на двойках.

Таким образом, надо сложить друг с другом те степени двойки, для которых в двоичной записи числа стоит единица. Например, нам нужно перевести в десятичную систему двоичное число «101100110».

Степень двойки	Двоичные разряды
256	1
128	0
64	1
32	1
16	0
8	0
4	1
2	1
1	0

Эта таблица показывает, как это сделать. Для этого надо сложить числа 256, 64, 32, 4 и

2, и у нас получится 358. Впрочем, когда ты научишься пользоваться двоичной системой счисления так же обыденно, как и десятичной, тебе не надо будет ничего никуда переводить – ты сможешь считать и выполнять все необходимые математические операции прямо в этой системе (кстати, она намного проще, чем десятичная).

Итак, теперь ты понимаешь, что для тех, кто умеет пользоваться двоичной системой счисления, «круглые» числа – это не 10, 100, 1000 и далее, а числа, которые в десятичной системе записываются так: 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024 и т. д. Запомни эти числа, они, можно сказать, «волшебные». Например, их очень часто используют программисты. Есть даже такой анекдот: программисты думают, что в километре 1024 метра, а в килограмме 1024 грамма, поскольку в килобайте – 1024 байта. И в этом есть доля правды: число 1024 в двоичной системе счисления записывается как единица с десятью нулями: 10000000000. (Это абсолютно «круглое» число: даже число его нулей – 10 – является круглым как в десятичной, так и в двоичной записи).

Есть и ещё одна шутка: ***в мире существует 10 типов людей – те, кто знает двоичную систему, и те, кто не знает её*** . Надеюсь, что теперь ты можешь посмеяться над ней вместе со мной, поскольку и ты теперь знаешь двоичную систему.

Вот тут необходимо остановиться и запомнить новый термин. Ты уже давно знаешь, что такое «цифра». Так вот двоичные цифры, то есть 0 и 1, называются *битами* . Когда ты услышишь слово «*бит* », то сразу поймешь, что речь идёт о двоичных цифрах.

Теперь вспомни, что мы договорились использовать в нашем специальном алфавите (который ввели на прошлой неделе) ровно 32 символа. Теперь ты понимаешь, почему на прошлой неделе я выделил слово «ровно»? Число 32 действительно «ровное» или «круглое», поскольку в двоичной системе счисления для его записи используется число 100000. Что это значит для нас? То, что для двоичного представления любого символа из нашего алфавита требуется пять двоичных цифр. Единственное, о чём нужно договориться: мы всегда будем использовать именно пять цифр, даже если в начале числа надо ставить нули: 00100, 01011 и т. д.

Таким образом можно закодировать все символы нашего алфавита от пробела до буквы «Я». Все они получают номер от 0 до 31 в десятичной системе счисления и код от 00000 до 11111 в двоичной. Вот интересная таблица, которую я рекомендую тебе выучить наизусть:

ПРОБЕЛ	0	00000	П	16	10000
А	1	00001	Р	17	10001
Б	2	00010	С	18	10010
В	3	00011	Т	19	10011
Г	4	00100	У	20	10100

Д	5	00101	Ф	21	10101
Е	6	00110	Х	22	10110
Ж	7	00111	Ц	23	10111
З	8	01000	Ч	24	11000
И	9	01001	Ш	25	11001
Й	10	01010	Щ	26	11010
К	11	01011	Ъ	27	11011
Л	12	01100	Ы	28	11100
М	13	01101	Э	29	11101
Н	14	01110	Ю	30	11110
О	15	01111	Я	31	11111

Это достаточно простое кодирование. По сути, это шифр одноалфавитной замены, то есть код, не скрывающий тайную информацию. Но что нам это даёт?

Давай вновь обратимся к полученному сообщению. Итак, в нём использованы обычные и жирные буквы. Что, если обычная буква обозначает «0», а жирная – «1»? Надо попробовать декодировать шифр таким способом. Если подставить цифры 0 и 1 вместо обычных и жирных букв, то получится вот такая кодограмма (я сразу же разделил *поток символов* на группы по пять цифр, чтобы было удобно, и тебе советую сразу научиться всегда делать именно так):

00010 00110 10001 00110 00100 01001 10010 11011 00000 00010 00001 00010 10100 11001 01011 10100 00000 01111 01110 00001 00000 01001 01110 01111 10000 01100 00001 01110 00110 10011 11111 01110 01011 00001

Оставляю тебе возможность потренироваться в раскодировании текста. Тем более что здесь его не так уж и много.

Чему же мы научились на этой неделе? Мы научились очень важной вещи. Оказывается, можно скрывать информацию в другой информации так, что найти её сможет только тот, кто знает, как искать. Это как спрятать иголку в стоге сена. Более того, в стогу вообще мало кто будет искать иголку! Добиться этого – и есть основная задача *стеганографии* , то есть науки о сокрытии информации. Если криптография шифрует смысл текста, то стеганография скрывает само присутствие тайны. Получается, криптография и стеганография – очень близкие науки. Одна прячет смысл сообщения, а другая – само сообщение. А метод, который мы с тобой сейчас изучаем, называется **методом Фрэнсиса Бэкона.**



Фрэнсис Бэкон – английский философ, историк, политик. Создал метод кодирования и сокрытия информации, из-за которого в дальнейшем произошло множество интересных случаев с поиском скрытых сообщений там, где их нет. Например, последователи этого метода пытались доказать, что все пьесы Уильяма Шекспира на самом деле были написаны Бэконом.

Ещё мы можем сделать вывод, что любое свойство, которое позволяет разделить буквы на два класса, можно использовать для сокрытия информации таким способом. Например, можно использовать заглавные и строчные буквы. Можно использовать чёрные и красные буквы. Можно, наконец, использовать не только обычное и жирное начертание, но и обычное и курсивное. Можно придумать ещё много всяких вариантов деления букв на два типа. К тому же при использовании нескольких способов деления вполне можно спрятать в одном и том же тексте несколько разных тайных сообщений. Например, одновременно использовать обычные и жирные буквы и заглавные и строчные буквы.

Рекомендую тебе потренироваться в кодировании и декодировании тайных сообщений таким способом. Это поможет хорошо понять изученный нами метод сокрытия информации. К тому же ты научишься свободно использовать двоичную систему счисления. Это в любом случае пригодится в будущем, кем бы тебе ни довелось стать.

Надо отметить, что профессиональный криптоаналитик всегда сможет обнаружить такие особенности текста, а потом сможет свободно декодировать тайное послание. На этот

способ нельзя надеяться, если скрыть информацию надо от того, кто знает о таком методе стеганографии. Теперь ты и сам о нем знаешь, а значит, как только увидишь странное сочетание символов с разным начертанием, сразу подумаешь о таком способе. Это касается и зашифрованного послания, то есть если скрытый текст подвергся не только кодированию двоичной системой, но и шифрованию каким-либо методом. Но об этом мы поговорим на следующей неделе.

Неделя 4. Операция XOR

На этой неделе я хочу научить тебя одной математической операции, которую не проходят в школе. Ведь в школе как? Сначала на уроках математики говорят, что есть только четыре математических операции – сложение, вычитание, умножение и деление. Потом оказывается, что это не математические операции, а только арифметические, и в старших классах добавляют к ним ещё три новых, математических – возведение в степень, вычисление корня и логарифма. А вдруг и это ещё не всё?

Да, действительно, не всё. Математики придумали огромное количество *операций* , которые можно производить над различными математическими объектами. И те операции над числами, которые изучают в школе, – лишь капля в океане чистого математического знания. Но мы не будем изучать весь океан, а рассмотрим только одну новую математическую операцию (которая очень нравится всем криптографам и криптоаналитикам). Эта операция называется «XOR», или, по-русски, «Исключающее ИЛИ», и обозначается значком ⊕. Ее выполняют не над числами, а над битами. На прошлой неделе мы уже выяснили, что такое бит – это «0» или «1».

Что ж, давай кратко изучим, что такое булевая логика, которая определяет операции над битами. Объектами в булевой логике являются биты, то есть два числа 0 и 1. Их можно рассматривать как значения истинности, когда 0 обозначает ЛОЖЬ, а 1 – ИСТИНА. Над такими значениями истинности определены различные операции. Например, самыми известными операциями являются НЕ (обозначается как ~), И (обозначается как ⊕) и ИЛИ (обозначается как |). У каждой операции есть так называемая таблица истинности. Рассмотрим их.

Операция НЕ:

~ 0 = 1

~ 1 = 0

Операция И:

0 ⊕ 0 = 0

0 ⊕ 1 = 0

1 ⊕ 0 = 0

1 ⊕ 1 = 1

Операция ИЛИ:

0 | 0 = 0

0 | 1 = 1

1 | 0 = 1

1 | 1 = 1

Вернёмся к операции ИСКЛЮЧАЮЩЕЕ ИЛИ, которая определяется очень просто. Выучи наизусть следующую таблицу истинности:

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

Эту операцию можно применять и к длинным двоичным числам. В этом случае она просто выполняется над каждым битом числа. Если выписать два двоичных числа в столбик друг под другом, то операция XOR выглядит очень просто:

$$\begin{array}{r} 01001 \\ \underline{11011} \\ 10010 \end{array}$$

Другими словами, операция XOR выполняется для каждого столбца по отдельности; тут нет необходимости переносить что-либо между разрядами числа, как это делается при сложении или умножении.

Чтобы лучше понять эту новую математическую операцию, можешь проделать такой опыт. Возьми монетку и подкинь её 100 раз (если ты хочешь схитрить и прочитать это число в двоичной системе счисления, чтобы делать меньше работы, то, так и быть, подкинь монетку 99 раз). Каждый раз записывай результат. «Орёл» обозначай битом 0, а «решка» – 1. Запиши это длинное число в одну строку. Во второй строке прямо под первым числом запиши это же самое число, но задом наперёд. Затем проведи длинную горизонтальную линию и под ней вычисли результат применения операции XOR к этим двум числам. Проверь себя: этот результат должен читаться одинаково как справа налево, так и слева направо. Сможешь объяснить почему?

А теперь я расскажу, почему эта операция так полюбилась криптографам. Всё просто. Пусть у тебя есть два различных числа – X и Y. Если применить операцию XOR к этим числам, то получится новое число $Z = (X \oplus Y)$. А если теперь к числу Z снова применить операцию XOR с числом Y, то результатом будет не что иное, как X!

Для примера давай вернемся к паре чисел, что мы рассматривали немного выше. Возьмем результат выполнения над ними операции XOR (10010), и теперь применим к нему эту операцию с тем же самым числом 11011:

$$\begin{array}{r} 10010 \\ \underline{11011} \\ 01001 \end{array}$$

Что получилось? Правильно, первое число – 01001.

Это важное *свойство обратимости* результата постоянно используется в криптографии. Давай посмотрим почему.

Напомню, что на прошлой неделе мы ввели новый алфавит, состоящий из тридцати двух символов, включая пробел. Каждому символу было сопоставлено пятизначное двоичное число от 00000 до 11111. Собственно, после этого уже было все понятно: мы же можем применять к кодам символов операцию XOR! Действительно, такое применение – просто другой способ использования шифра подстановки. Но этот способ намного проще: не надо искать соответствия в таблицах, а можно просто применить операцию XOR. Причём и для шифрования, и для расшифровки необходимы одинаковые действия.

Давай рассмотрим этот процесс на примере. Пусть нам необходимо зашифровать слово «ОГОНЬ». В качестве ключа возьмём единственную букву «Р». Вот что получится:

Текст:	**О**	**Г**	**О**	**Н**	**Ь**
	01111	00100	01111	01110	11011
Ключ: Р	10001	10001	10001	10001	10001
Резуль-	11110	10101	11110	11111	01010
тат:	**Ю**	**Ф**	**Ю**	**Я**	**Й**

Так из слова «ОГОНЬ» получилось слово «ЮФЮЯЙ». Расшифровка происходит таким же образом:

Шифро-	**Ю**	**Ф**	**Ю**	**Я**	**Й**
грамма:	11110	10101	11110	11111	01010
Ключ: Р	10001	10001	10001	10001	10001
Резуль-	01111	00100	01111	01110	11011
тат:	**О**	**Г**	**О**	**Н**	**Ь**

Математически это можно записать так: «ОГОНЬ ⊕ РРРРР = ЮФЮЯЙ» и «ЮФЮЯЙ ⊕ РРРРР = ОГОНЬ». Как ты понимаешь, сейчас мы использовали просто шифр подстановки с одноалфавитной заменой. Это неинтересно. Интересно здесь то, что шифрование и расшифровка происходят при помощи одного и того же действия.

Теперь рассмотрим иной пример. Пусть нам опять надо зашифровать слово «ОГОНЬ», но теперь в качестве ключа мы будем использовать слово «МАГИЯ». Что получится? А вот что:

Текст:	**О**	**Г**	**О**	**Н**	**Ь**
	01111	00100	01111	01110	11011
Ключ:	**М**	**А**	**Г**	**И**	**Я**
	01101	00001	00100	01001	11111
Ре-	00010	00101	01011	00111	00100
зуль-тат:	**Б**	**Д**	**К**	**Ж**	**Г**

Абсолютно так же производится расшифровка:

Текст:	Б	Д	К	Ж	Г
	00010	00101	01011	00111	00100
Ключ:	М	А	Г	И	Я
	01101	00001	00100	01001	11111
Ре-зуль-тат:	01111	00100	01111	01110	11011
	О	Г	О	Н	Ь

Получается, что мы теперь можем «складывать» друг с другом целые слова: «ОГОНЬ ⊕ МАГИЯ = БДКЖГ». Это действительно какая-то магия. Только что мы при помощи этой прекрасной операции XOR применили шифр многоалфавитной замены, который изучали на второй неделе. Одна и та же операция позволяет применять сразу два шифра, которые мы уже изучили. Это прекрасно!

Само собой разумеется, этот процесс можно упростить. Ведь очевидно, что результат применения операции XOR никогда не меняется. Поэтому можно запросто составить таблицу вроде той, которую мы сделали на второй неделе, только теперь в ячейках на пересечении строк и столбцов будут буквы, получающиеся в результате применения операции XOR. Вот такая таблица получается: (см. на следующем развороте).

У этой таблицы много примечательных свойств. Если ты внимательно её изучишь, то найдёшь в ней разнообразные закономерности. Обрати, например, внимание на то, как в таблице располагаются буквы А, В, Ж, О и Я, а потом посмотри на их двоичное представление. И таких узоров в ней большое количество. Это – следствие разных свойств, которыми обладают двоичные числа и двоичная система счисления.

Теперь давай потренируемся. Итак, у тебя есть послание следующего вида:

«ПРИВеТ МОЙ ДороГОй ДРУГ СеГОдНЯ Я хОЧу РАССКаЗаТь ТЕбе оДну ЗаниМАТеЛьНуЮ ИстоРию КОТОрАЯ СлучилАСЬ сО МНоЙ мНого Лет НАзад КоГДА я бЫЛ Ещё СОвСем мАЛЕНьким Я ТоГдА Жил в ДаЛёкОй ДЕРевНЕ и БЫл нАмноГо БЛИЖЕ к пРИрОДе чем СЕЙЧАс и ВоТ Однажды я шёл по лесу и увидел за деревьями яркий красный свет также было слышно странное жужжание подкравшись поближе я увидел марсиан».

		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я
		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я
А	А		В	Б	Д	Г	Ж	Е	И	З	К	Й	М	Л	О	Н	Р	П	Т	С	Ф	У	Ц	Х	Ш	Ч	Ъ	Щ	Э	Ы	Я	Ю
Б	Б	В		А	Е	Ж	Г	Д	Й	К	З	И	Н	О	Л	М	С	Т	П	Р	Х	Ц	У	Ф	Щ	Ъ	Ч	Ш	Ю	Я	Ы	Э
В	В	Б	А		Ж	Е	Д	Г	К	Й	И	З	О	Н	М	Л	Т	С	Р	П	Ц	Х	Ф	У	Ъ	Щ	Ш	Ч	Я	Ю	Э	Ы
Г	Г	Д	Е	Ж		А	Б	В	Л	М	Н	О	З	И	Й	К	У	Ф	Х	Ц	П	Р	С	Т	Ы	Э	Ю	Я	Ч	Ш	Щ	Ъ
Д	Д	Г	Ж	Е	А		В	Б	М	Л	О	Н	И	З	К	Й	Ф	У	Ц	Х	Р	П	Т	С	Э	Ы	Я	Ю	Ш	Ч	Ъ	Щ
Е	Е	Ж	Г	Д	Б	В		А	Н	О	Л	М	Й	К	З	И	Х	Ц	У	Ф	С	Т	П	Р	Ю	Я	Ы	Э	Щ	Ъ	Ч	Ш
Ж	Ж	Е	Д	Г	В	Б	А		О	Н	М	Л	К	Й	И	З	Ц	Х	Ф	У	Т	С	Р	П	Я	Ю	Э	Ы	Ъ	Щ	Ш	Ч
З	З	И	Й	К	Л	М	Н	О		А	Б	В	Г	Д	Е	Ж	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	П	Р	С	Т	У	Ф	Х	Ц
И	И	З	К	Й	М	Л	О	Н	А		В	Б	Д	Г	Ж	Е	Ш	Ч	Ъ	Щ	Э	Ы	Я	Ю	Р	П	Т	С	Ф	У	Ц	Х
Й	Й	К	З	И	Н	О	Л	М	Б	В		А	Е	Ж	Г	Д	Щ	Ъ	Ч	Ш	Ю	Я	Ы	Э	С	Т	П	Р	Х	Ц	У	Ф
К	К	Й	И	З	О	Н	М	Л	В	Б	А		Ж	Е	Д	Г	Ъ	Щ	Ш	Ч	Я	Ю	Э	Ы	Т	С	Р	П	Ц	Х	Ф	У
Л	Л	М	Н	О	З	И	Й	К	Г	Д	Е	Ж		А	Б	В	Ы	Э	Ю	Я	Ч	Ш	Щ	Ъ	У	Ф	Х	Ц	П	Р	С	Т
М	М	Л	О	Н	И	З	К	Й	Д	Г	Ж	Е	А		В	Б	Э	Ы	Я	Ю	Ш	Ч	Ъ	Щ	Ф	У	Ц	Х	Р	П	Т	С
Н	Н	О	Л	М	Й	К	З	И	Е	Ж	Г	Д	Б	В		А	Ю	Я	Ы	Э	Щ	Ъ	Ч	Ш	Х	Ц	У	Ф	С	Т	П	Р
О	О	Н	М	Л	К	Й	И	З	Ж	Е	Д	Г	В	Б	А		Я	Ю	Э	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р	П
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	Р	П	Т	С	Ф	У	Ц	Х	Ш	Ч	Ъ	Щ	Э	Ы	Я	Ю	А		В	Б	Д	Г	Ж	Е	И	З	К	Й	М	Л	О	Н
С	С	Т	П	Р	Х	Ц	У	Ф	Щ	Ъ	Ч	Ш	Ю	Я	Ы	Э	Б	В		А	Е	Ж	Г	Д	Й	К	З	И	Н	О	Л	М
Т	Т	С	Р	П	Ц	Х	Ф	У	Ъ	Щ	Ш	Ч	Я	Ю	Э	Ы	В	Б	А		Ж	Е	Д	Г	К	Й	И	З	О	Н	М	Л
У	У	Ф	Х	Ц	П	Р	С	Т	Ы	Э	Ю	Я	Ч	Ш	Щ	Ъ	Г	Д	Е	Ж		А	Б	В	Л	М	Н	О	З	И	Й	К
Ф	Ф	У	Ц	Х	Р	П	Т	С	Э	Ы	Я	Ю	Ш	Ч	Ъ	Щ	Д	Г	Ж	Е	А		В	Б	М	Л	О	Н	И	З	К	Й
Х	Х	Ц	У	Ф	С	Т	П	Р	Ю	Я	Ы	Э	Щ	Ъ	Ч	Ш	Е	Ж	Г	Д	Б	В		А	Н	О	Л	М	Й	К	З	И
Ц	Ц	Х	Ф	У	Т	С	Р	П	Я	Ю	Э	Ы	Ъ	Щ	Ш	Ч	Ж	Е	Д	Г	В	Б	А		О	Н	М	Л	К	Й	И	З
Ч	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	П	Р	С	Т	У	Ф	Х	Ц	З	И	Й	К	Л	М	Н	О		А	Б	В	Г	Д	Е	Ж
Ш	Ш	Ч	Ъ	Щ	Э	Ы	Я	Ю	Р	П	Т	С	Ф	У	Ц	Х	И	З	К	Й	М	Л	О	Н	А		В	Б	Д	Г	Ж	Е
Щ	Щ	Ъ	Ч	Ш	Ю	Я	Ы	Э	С	Т	П	Р	Х	Ц	У	Ф	Й	К	З	И	Н	О	Л	М	Б	В		А	Е	Ж	Г	Д
Ъ	Ъ	Щ	Ш	Ч	Я	Ю	Э	Ы	Т	С	Р	П	Ц	Х	Ф	У	К	Й	И	З	О	Н	М	Л	В	Б	А		Ж	Е	Д	Г
Ы	Ы	Э	Ю	Я	Ч	Ш	Щ	Ъ	У	Ф	Х	Ц	П	Р	С	Т	Л	М	Н	О	З	И	Й	К	Г	Д	Е	Ж		А	Б	В
Э	Э	Ы	Я	Ю	Ш	Ч	Ъ	Щ	Ф	У	Ц	Х	Р	П	Т	С	М	Л	О	Н	И	З	К	Й	Д	Г	Ж	Е	А		В	Б
Ю	Ю	Я	Ы	Э	Щ	Ъ	Ч	Ш	Х	Ц	У	Ф	С	Т	П	Р	Н	О	Л	М	Й	К	З	И	Е	Ж	Г	Д	Б	В		А
Я	Я	Ю	Э	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Е	Д	Г	В	Б	А	

Как ты уже понимаешь, на самом деле здесь два текста. Первый текст – это «обманка», призванная затуманить секрет. Странная история про марсиан. На самом-то деле скрытое послание закодировано в размере букв. Так как конец текста полностью состоит из строчных букв, можно предположить, что именно строчная буква обозначает бит 0. А заглавная буква, соответственно, обозначает бит 1. Если ты тщательно проделаешь операцию декодирования, то должно получиться следующее:

11110 11111 00011 01111 10110 11101 10111 11010 10110 00100 10001 11010 10110 00100 11110 11100 00011 10111 01010 00100 11000 10111 00111 00110 10001 11100 00110 10110 00101 11001 10110 01000 10111 11001 10110 00011 11100 10110

Использование уже известной тебе таблицы для преобразования двоичных чисел в буквы даёт такой текст:

«ЮЯВОХЭЦЩХГРЩХГЮЫВЦЙГЧЦЖЕ РЫЕХДШХЗЦШХВЫХ».

На первый взгляд выглядит странно, и первая мысль, которая приходит в голову, – возможно, в процессе декодирования мы допустили ошибку.

Но вдруг это закодированная шифрограмма? Что, если автор послания использовал метод стеганографии для сокрытия не простого текста, а зашифрованного? Почему бы и нет? Это вполне возможно. Что же тут можно сделать?

Помнишь, как на второй неделе мы оценивали шифр при помощи гистограммы частот символов? Конечно, на таком малом объёме текста нормально посчитать частоты затруднительно. Но тем не менее, если ты это сделаешь, а потом построишь гистограмму, то

увидишь, что она примерно соответствует гистограмме частот символов в русском языке. Значит, перед нами шифр одноалфавитной замены!

Как быть дальше? Есть три возможных пути:

1. Провести частотный анализ, как мы делали это на первой неделе. Это универсальный путь, он всегда дает решение.

2. Поскольку мы столкнулись с двоичным кодированием символов, спрятанных потом в тексте-обманке, то резонно предположить, что для шифрования воспользовались операцией XOR. Так что можно последовательно проверить каждый код из тридцати одного (первый код проверять смысла нет, это код 00000, соответствующий пробелу, он не меняет текста). В итоге ты найдёшь тот код, которым зашифровано послание. Попробуй.

3. А можно поступить ещё более хитро и объединить эти два метода. Самый частый символ в тексте на русском языке – пробел. В шифрограмме самый частый встречающийся символ – Х. Однако Х стоит в конце шифрограммы, так что вряд ли это пробел (какой резон ставить пробел в конец текста?). Второй по частоте символ в шифрограмме – Ц. В таких коротких текстах часто случается, что символы меняются местами по частоте. Так что попробуй применить операцию XOR к шифрограмме с ключом Ц.

Если ты всё правильно сделал, то в результате должен получиться текст «ИЗУЧАЙ МАТЕМАТИКУ ЭТО ПРЕКРАСНАЯ НАУКА». По-моему, это отличное послание для любого человека.

Теперь ты можешь придумать какое-нибудь послание и попробовать зашифровать его подобным образом (лучше в качестве ключа использовать не очень длинное слово). Это будет очень хорошее упражнение как для тренировки описанного метода шифрования, так и для изучения криптографии в целом. Так что рекомендую сделать следующее:

1. Придумай текст, который ты хочешь зашифровать, длиной не менее 50 символов.

2. Придумай секретный ключ, при помощи которого ты будешь шифровать текст.

3. Теперь придумай открытое сообщение длиной не менее 250 символов (помни, что для кодирования одного символа тайного текста требуется 5 символов открытого сообщения).

4. Зашифруй тайное послание при помощи ключа, используя для этого операцию XOR.

5. Теперь закодируй полученную шифрограмму методом Фрэнсиса Бэкона (который мы изучили на прошлой неделе).

Пошли это письмо кому-нибудь (например, мне по адресу *roman.dushkin@gmail.com*).

После того как ты выполнишь это непростое упражнение, ты сможешь уверенно пользоваться изученным на этой неделе методом шифрования. И это будет хорошо.

Неделя 5. Тарабарская грамота

Теперь давай изучим немного иной подход к тайной переписке. Мы будем использовать то, что потенциальный взломщик не знает, как именно зашифрован секретный текст. Это значит, что альтернатив и возможностей для проверки у него слишком много. Всё дело в том, что участники обмена сообщениями должны заранее договориться о том, какой метод шифрования или сокрытия информации они будут использовать. Если сам метод сложно

распознать по виду текста, то криптоаналитик может голову сломать, но не разобраться в секрете.

Заметь: всё, что мы изучили до сих пор, не подходит под это понимание. Если мы используем шифр одноалфавитной замены, то это можно понять по самому виду текста. Более того, частотный анализ с построением гистограммы сразу же полностью раскрывает метод шифрования (и мы с тобой уже тоже научились это делать). С многоалфавитной заменой – всё то же самое. Достаточно только предположить, что текст зашифрован при помощи многоалфавитной замены, чтобы применить к нему метод расшифровки, который мы использовали на второй неделе. И если этот метод найдёт длину ключа, то тайна сразу же перестаёт быть тайной.

То же самое подходит и к сокрытию информации при помощи двоичного кодирования через свойства символов. Как только криптоаналитик видит, что символы в тексте отличаются друг от друга как-то регулярно, он сразу же предполагает: в деле замешана двоичная система счисления, после чего начинает искать закономерности. В конце концов, шифр поддаётся, тайна раскрыта.

Другими словами, если криптоаналитик узнаёт метод шифрования, получение открытого текста из шифрограммы становится делом техники и очень внимательных и точных подсчётов. Но на этой неделе мы изучим пару методов, которые в целом лишены такого недостатка.

Если два человека хотят обмениваться секретными сообщениями так, чтобы их никто не понял, у них есть для этого два способа. Первый заключается в том, чтобы воспользоваться широко известными алгоритмами или методами шифрования, более или менее стойкими к взлому. Поскольку описание методов известно, то нет никаких проблем в том, чтобы использовать их.

Второй способ заключается в использовании метода, который не будет известен никому, кроме участников обмена тайной информацией. Само собой разумеется, что договориться о таком методе и обменяться разного рода ключами необходимо заранее – то есть требуется двойной обмен информацией. В первый раз необходимо встретиться лично и тайно, чтобы обменяться ключами и методами шифрования. Потом уже можно пересылать друг другу информацию по открытым каналам, не опасаясь, что тайны будут раскрыты.

На этой неделе мы изучим метод, который получил название «Тарабарская грамота». Слово «тарабарский» обозначает «непонятный», «бессмысленный». Тарабарский язык – это речь, составленная из бессмысленного набора звуков, часто подражающая какому-либо известному языку или даже нескольким языкам. Например, известную фразу «Глокая куздра штеко будланула бокра и курдячит бокрёнка» можно считать фразой на тарабарском языке, при этом построенной по правилам русского.

Или, например, попробуй расшифровать, что написано в этом тексте:

RIП ZWON ЛУJVU IЧLИSS JЛWOZR CIILЬ QУPWAN

Если у тебя ничего не выходит, и никаких идей в голову не приходит, то попробуй вычеркнуть из этого набора букв те, которые не входят в русский алфавит. Получилось?

Но это очень просто. Есть методы куда более сложные. Их использование требует больших усилий, поскольку надо очень внимательно подбирать слова и фразы так, чтобы у криптоаналитика не было возможности за что-то зацепиться. Например, составить скрытое сообщение так, чтобы читать нужно было только третью букву каждого слова, если в слове

три или больше букв. Понятное дело, что тут надо очень тщательно выбирать слова – так, чтобы у текста был смысл, и смысл этот был вполне нормальный, а не абы какой. Если в тексте попадаются какие-то несуразности – это первый признак того, что такое сообщение предназначено для наведения тумана, а истинная информация передаётся внутри этого сообщения тайно.

Для тренировки можно выполнить такие упражнения. Придумай какое-нибудь слово, не короткое и не длинное. Например, это может быть слово «ПЛАМЯ». Теперь тебе надо придумать фразу из пяти слов, которые начинаются на буквы «П», «Л», «А», «М», и «Я». Например: «Подо Льдом Араб Мучил Янычара». Теперь ты понимаешь, что такое неадекватность текста? А теперь придумай фразу из пяти слов, где слово «ПЛАМЯ» будет читаться по вторым буквам. Например: «сПособ пЛавания рАзработан уМным дЯдей». Как видишь, эта задача не так проста, как кажется на первый взгляд, и здесь требуются многочисленные тренировки.

Но это всё ещё не очень хороший метод. Давай замахнёмся на что-нибудь посерьёзней. Представь, что тебе в руки попала следующая шифрограмма:

ARK NANTONG CELL TREC ISOHY KNAV BAR IPS EXES PISIDIE UXQUELS HABEN KANBUN WORLD BE XERM SOME TEXIS YRS BELLIC

На первый взгляд она выглядит как довольно странный набор английских слов, многие из которых – очень редкие и встречаются только в специализированной литературе, а некоторые вообще написаны с ошибками. Сразу же приходит на ум вычленить из этого бессмысленного набора символов только те, которые похожи своим начертанием на буквы русского алфавита (таких букв 12: A, B, C, E, H, K, M, O, P, T, X, Y). Вот что получается:

AKATOCETECOHYKABAPEXEPEXEHABEKABOBEXEMOMETEXYBEC

Что с этим делать дальше? Здесь я рекомендую тебе прервать дальнейшее чтение и попробовать самостоятельно найти в этом наборе букв какие-либо закономерности. Попробуй «загрузить» эту последовательность к себе в голову, после чего погоняй её туда-сюда день или два. Если ничего не получится найти, то продолжай чтение. Если получится, то сравни свой результат с тем, что написано дальше.

1. В этой строке на нечётных местах всегда стоит буква, обозначающая гласную, а на чётных – согласную. Другими словами, гласные и согласные идут одна за другой.

2. Различных гласных четыре: A, E, O, Y. Согласных – восемь: B, C, H, K, M, P, T, X. Произведение 4 и 8 даёт 32.

3. Прошлые две недели мы использовали алфавит, содержащий 32 символа.

Не много ли совпадений для такого небольшого кусочка шифрованного текста? Действительно, многовато. Это значит, что их нужно проверить. Ведь криптоаналитик всегда пытается зацепиться за разного рода закономерности. Когда в шифрограмме обнаруживаются закономерности, это значит, что она потенциально поддается взлому. Самый неуязвимый шифр похож на «*белый шум*» – никаких закономерностей, абсолютный хаос.

Давай попробуем проверить догадку, которая заключается в том, что в представленной шифрограмме за каждый символ секретного текста отвечают сразу гласная и согласная. При этом 32 символа нашего алфавита можно разделить на четыре группы, и каждую группу

обозначить гласной. Внутри же групп символы (которых по восьми в группе) обозначаются согласными. Таким образом, чтобы получить код символа, надо взять гласную его группы и согласную самого символа в группе. Предположим, что кодировка была простейшей (если нет, то необходимо применить частотный анализ, используя в качестве символов, частоты которых подсчитываются, пары букв «Гласная + Согласная»). Простейшая кодировка обозначает, что гласные и согласные использовались просто по порядку. В итоге получается такая таблица:

ПРОБЕЛ	AB	**З**	EB	**П**	OB	**Ч**	YB
А	AC	**И**	EC	**Р**	OC	**Ш**	YC
Б	AH	**Й**	EH	**С**	OH	**Щ**	YH
В	AK	**К**	EK	**Т**	OK	**Ъ**	YK
Г	AM	**Л**	EM	**У**	OM	**Ы**	YM
Д	AP	**М**	EP	**Ф**	OP	**Э**	YP
Е	AT	**Н**	ET	**Х**	OT	**Ю**	YT
Ж	AX	**О**	EX	**Ц**	OX	**Я**	YX

Думаю, тебя не затруднит с её помощью расшифровать то, что было скрыто в том беспорядочном наборе английских слов.

Теперь давай подумаем, как можно усложнить этот способ шифрования так, чтобы потенциальному взломщику было труднее обнаружить и взломать его. На ум приходит несколько идей. Во-первых, надо сделать так, чтобы английский текст был более похож на обычную человеческую речь. Во-вторых, не должно быть такой простейшей закономерности, как та, которую мы обнаружили ранее: чередования гласных и согласных. Предлагаю попробовать избавиться от обоих недостатков.

Проще всего сразу же избавиться от второго нюанса. По крайней мере, это будет не так явно видно, как в рассмотренном нами случае. Почему бы не сделать произвольным порядок букв в коде? Какая разница, как записывать: «AT» или «TA» – это будет обозначать одно и то же. Главное, что при расшифровке мы отбираем по две буквы и переводим их в символ скрытого текста. Можно было бы и ещё сильнее усложнить эту сторону задачи, но это связано с серьёзными техническими сложностями (слишком много вычислений), поэтому такое усовершенствование я оставляю тебе в качестве самостоятельной работы.

Теперь давай займёмся первой проблемой. Она возникает из-за того, что в шифрограмме встречаются очень неудобные с точки зрения английского языка сочетания букв, для которых надо подбирать слова, а слов с такими сочетаниями либо нет вообще, либо очень мало. Частично эта проблема будет решена уже при разрешении использовать сочетания двух букв в произвольном порядке (предыдущая задача). Но можно пойти дальше.

Если помнишь, на первой неделе мы изучали частотный анализ и узнали о таблице частот встречаемости русских букв в текстах. Как ты понимаешь, такую же таблицу можно составить и для английского языка. Вот она:

Буква	**Частота %**	**Буква**	**Частота %**	**Буква**	**Частота %**	**Буква**	**Частота %**
E	12,70	H	6,09	M	2,41	V	0,98
T	9,06	R	5,99	W	2,36	K	0,77
A	8,17	D	4,25	F	2,23	X	0,15
O	7,51	L	4,03	G	2,02	J	0,15
I	6,97	C	2,78	Y	1,97	Q	0,10
N	6,75	U	2,76	P	1,93	Z	0,05
S	6,33			B	1,49		

И у нас есть частоты встречаемости букв русского алфавита в тексте. Их можно совместить так, чтобы наиболее часто встречающимся русским буквам соответствовали наиболее часто встречающиеся пары английских букв. Для этого надо рассчитать частоты для пар. Это сделать просто – чтобы получить частоту для пары, достаточно перемножить частоты двух букв (честно говоря, это не совсем корректно с точки зрения языка, но для нашей задачи подойдёт). Выбрав только латинские буквы A, B, C, E, H, K, M, O, P, T, X, Y, мы получим следующую таблицу:

	A (8,17)	E (12,70)	O (7,51)	Y (1,97)
B (1,49)	12,1733	18,923	11,1899	2,9353
C (2,78)	22,7126	35,306	20,8778	5,4766
H (6,09)	49,7553	77,343	45,7359	11,9973
K (0,77)	6,2909	9,779	5,7827	1,5169
M (2,41)	19,6897	30,607	18,0991	4,7477
P (1,93)	15,7681	24,511	14,4943	3,8021
T (9,06)	74,0202	115,062	68,0406	17,8482
X (0,15)	1,2255	1,905	1,1265	0,2955

Теперь надо расположить двухбуквенные комбинации по убыванию их частоты:

ET EH AT OT AH OH EC EM EP AC OC AM EB OM YT AP OP AB YH OB EK AK OK YC YM YP YB EX YK AX OX YX

Как ты можешь подсчитать, тут ровно 32 пары букв, и теперь мы можем сопоставить их буквам русского алфавита, выстроив по уменьшению частоты. Получается вот такая замечательная таблица (попробуй сначала составить её самостоятельно, а потом сравни):

ПРОБЕЛ	ET	**З**	OB	**П**	YT	**Ч**	OK
А	OT	**И**	AH	**Р**	AC	**Ш**	YB
Б	AK	**Й**	YC	**С**	EM	**Щ**	AX
В	OC	**К**	AM	**Т**	EC	**Ъ**	YH
Г	EK	**Л**	EP	**У**	AP	**Ы**	AB
Д	OM	**М**	EB	**Ф**	YX	**Э**	YK
Е	AT	**Н**	OH	**Х**	YP	**Ю**	EX
Ж	YM	**О**	EH	**Ц**	OX	**Я**	OP

Давай попробуем зашифровать что-нибудь с помощью этого кода. Так, фраза «ПРИЕДУ ЗАВТРА» в переложении на код будет выглядеть так: «YTACAHATOMAPETOBOTOCECACOT». Теперь, зная, что в двухбуквенных сочетаниях буквы можно менять местами, попробуй подобрать английские слова для сокрытия этой шифрограммы.

Если попытаться сделать это, то может получиться что-то вроде такого:

STYLUS CALLAHAN TROMP ARES TOROID BIT ROW CENSUS CARD CITO

Подобрать этот набор слов было намного-намного проще, чем предыдущий (мне даже практически не пришлось открывать словарь). Выглядит этот набор как список каких-то слов, возможно, кодов. Криптоаналитик будет ломать над ним голову намного дольше, поскольку здесь нет необычностей.

Я рекомендую тебе потренироваться этому методу, и если ты неплохо знаешь английский язык, то попробуй самостоятельно что-нибудь зашифровать и отправить человеку, с которым ты переписываешься по теме криптографии. Посмотрим, как он удивится.

Напоследок – пара советов:

1. Чем больше в системе шифрования закономерностей, тем проще криптоаналитику расшифровать шифрограмму. Поэтому любыми средствами избегай простых закономерностей, которые позволят зацепиться за них и распутать клубок тайны.

2. Чем необычнее текст, тем больше подозрений он вызовет у криптоаналитика, который будет искать скрытую информацию. Поэтому для сокрытия важной информации пользуйся как можно более простыми и обычными текстами.

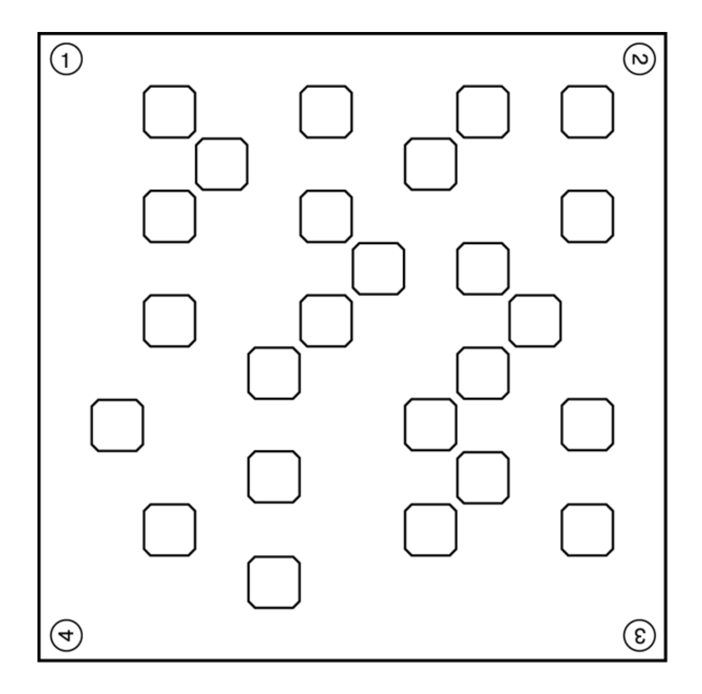
Вот и всё. До следующей недели.

Неделя 6. Шифрование дырявой матрицей

Теперь давай научимся новому методу шифрования. Он основан не на замене символов, а на их перемешивании. Ведь если перемешать текст, то воссоздать его будет очень сложно. Например, если просто выписать все буквы текста в алфавитном порядке, то расположить их правильно будет очень непросто. Например, что может быть тут зашифровано: АААА ВВВ ДД ЕЕЕ ИИИ Й МММ ННН ОООО П РР С ТТ УУУ Ф Ч Ш Ь ЯЯ? А ведь это просто все буквы первого предложения этого абзаца, упорядоченные по алфавиту.

Но подобные перестановки бессмысленны, поскольку для их расшифровки требуется информация о расстановке символов в правильном порядке, а это практически то же самое, что и запись самой фразы. Так что мы изучим иной способ перестановок. Ключ для них представляет собой квадрат с вырезанными в нём отверстиями. Это настоящий, материальный «ключ», поскольку его можно взять в руки и повертеть. И этот метод шифрования называется «решётка Кардано».

Представь себе квадрат, вырезанный из бумаги. Примерно такой:



Если ты внимательно приглядишься, то увидишь в углах этого квадрата четыре цифры. Ими обозначена последовательность применения этого ключа.

Теперь попробуй сделать ключ своими руками. Возьми лист бумаги в клетку, например, из тетради, и вырежи из него квадрат 12 × 12 клеток. Затем обведи внутри квадрата «границу» шириной в 1 клетку. После этого внутренний квадрат будет размером в 10 10 клеток. Теперь тщательно перенеси на свою заготовку квадратики с рисунка в книге. Затем надо будет очень аккуратно вырезать эти квадратики. Для этого подойдет канцелярский нож или лезвие, но лучше попросить о помощи кого-либо из взрослых.

С этим ключом ты сможешь шифровать и расшифровывать тексты. С ним работают так: положи ключ на лист бумаги так, чтобы в верхнем левом углу стояла цифра «1», после чего обведи края ключа. На листе бумаги появится квадрат. Далее в отверстия в ключе надо вписать по одной букве текст, который хочешь зашифровать (пробелы, кстати, не пиши, их потом без проблем можно будет восстановить). Когда все квадратики будут заполнены, поверни ключ на 90 градусов против часовой стрелки так, чтобы в верхнем левом углу оказалась цифра «2». Если ты тщательно перенёс отверстия с рисунка на свой ключ, то ни одной буквы из написанных тобой видно не будет. Можно продолжать вписывать буквы в отверстия. Проделай это ещё дважды – для цифр «3» и «4». Всего этот ключ позволяет перемешать 100 букв текста.

Как только буквы перемешаны, возьми чистый лист бумаги и выпиши из квадрата 10 × 10 клеток полученные строчки, но уже обычным сплошным текстом во всю длину строки. Соответственно, чтобы расшифровать текст, надо взять строку и записать её в виде квадрата 10 × 10 клеток, после чего воспользоваться ключом для чтения. Несложно, не правда ли?



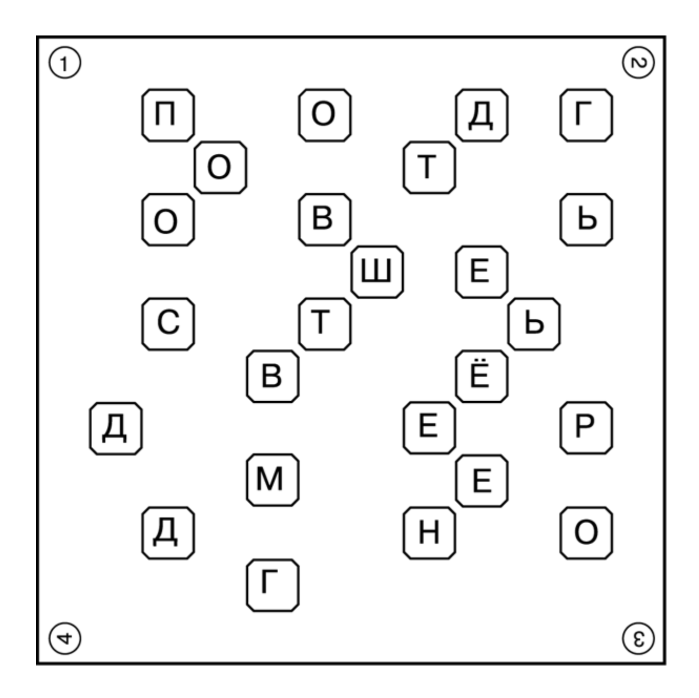
Джероламо Кардано – итальянский математик, инженер, философ и медик. Придумал много всякой всячины (в его честь названы формулы решения кубического уравнения, карданов подвес, карданный вал и решётки Кардано). Свою решётку Дж. Кардано предложил в 1550 году, и он планировал маскировать тайное сообщение под обычное письмо, а ключ представлял собой таблицу-карточку с вырезанными ячейками.

Давай потренируемся. Пусть необходимо зашифровать такой текст:

«ПОДГОТОВЬ ШЕСТЬ ВЁДЕР МЕДНОГО КУПОРОСА ВМЕСТЕ С ДОКУМЕНТАМИ И ВСЕМ ОСТАЛЬНЫМ НЕОБХОДИМЫМ К НАЧАЛУ СЛЕДУЮЩЕГО МЕСЯЦА».

В этой фразе ровно 100 букв (без пробелов), и мы можем без труда воспользоваться нашим ключом.

Итак, кладём ключ так, чтобы в верхнем левом углу была цифра «1», и начинаем вписывать буквы по порядку. Получается вот что:



Ну и так далее. Надеюсь, что остальные буквы ты сможешь вписать самостоятельно. Главное, забудь о пробелах. Они в данном методе не нужны и даже вредны, поскольку по ним криптоаналитик может попытаться восстановить открытый текст. Всегда помни: чем больше регулярности и закономерностей можно обнаружить в шифрограмме, тем проще её взломать. А поскольку пробел – самый часто встречаемый символ, то он вреден.

В итоге у тебя должна получиться такая матрица размером 10 × 10 букв:

О	П	К	Ы	О	М	У	Д	П	Г
И	М	О	И	О	К	Т	Н	В	А
Р	О	С	О	В	С	Е	А	Ч	Ь
М	В	А	О	Л	Ш	М	Е	Е	С
У	С	Т	С	Т	С	А	Л	Ь	Е
Т	Л	Е	В	С	Ь	Д	Ё	Н	Д
Д	У	Ы	Ю	М	О	Е	К	Щ	Р
Н	У	Е	М	Г	Е	О	Е	О	М
М	Д	Е	Б	Н	Е	Н	Х	Т	О
О	С	Д	Я	Г	И	А	Ц	М	А

Эту матрицу мы теперь выписываем в строку и получаем:

«ОПКЫОМУДПГИМОИОКТНВАРОСОВ СЕАЧЬМВАОЛШМЕЕСУСТСТСАЛЬЕТ ЛЕВСЬДЁНДДУЫЮМОЕКЩРНУЕМГЕОЕ ОММДЕБНЕНХТООСДЯГИАЦМА».

Согласись, что расшифровать такую перестановку практически невозможно.

Этот метод был придуман ещё в Средневековье и очень часто использовался по двум причинам: во-первых, он очень лёгок в применении, а во-вторых, разгадать зашифрованный текст без ключа практически невозможно.

Методы его расшифровки направлены скорее на добычу ключа, а не на попытки обнаружить какие-либо закономерности в этом хаосе букв. Пытаться переставлять буквы, чтобы найти какой-либо смысл, бесполезно: в процессе будут появляться многочисленные слова и даже небольшие фразы, которые не имеют никакого отношения к первоначально зашифрованному тексту. Можешь попробовать составлять слова из букв шифрограммы – их получится ну просто огромное количество.

Думаю, что на этой неделе ты получишь письмо, где будет такая шифровка. Можешь даже не пытаться расшифровывать её, просто ищи ключ. Когда найдёшь, сможешь прочитать.

После этого рекомендую тебе выполнить такое упражнение:

1. Придумай свой ключ в виде квадратной матрицы с отверстиями. Потренируйся, через некоторое время у тебя будет хорошо получаться.

2. Зашифруй какой-нибудь текст методом, описанным в этой книге на текущей неделе.

3. Отправь шифрограмму тому, кто посылает тебе письма, но ключ не отправляй.

Неделя 7. Древние и экзотические алфавиты

Вот и прошла половина лета и половина наших занятий. А это значит, что пора немного отдохнуть. Так что на этой неделе мы не будем заниматься математикой, а сменим тему и обратимся к истории и языкознанию. Но если ты думаешь, что это неинтересно, то зря. Между прочим, лингвистика (или языкознание) – это строгая наука, которая относится скорее к математической, нежели к гуманитарной области знаний. В лингвистике используется очень много математических методов, а в основе современной лингвистики лежит отрасль математики, которая называется *теорией формальных грамматик*.

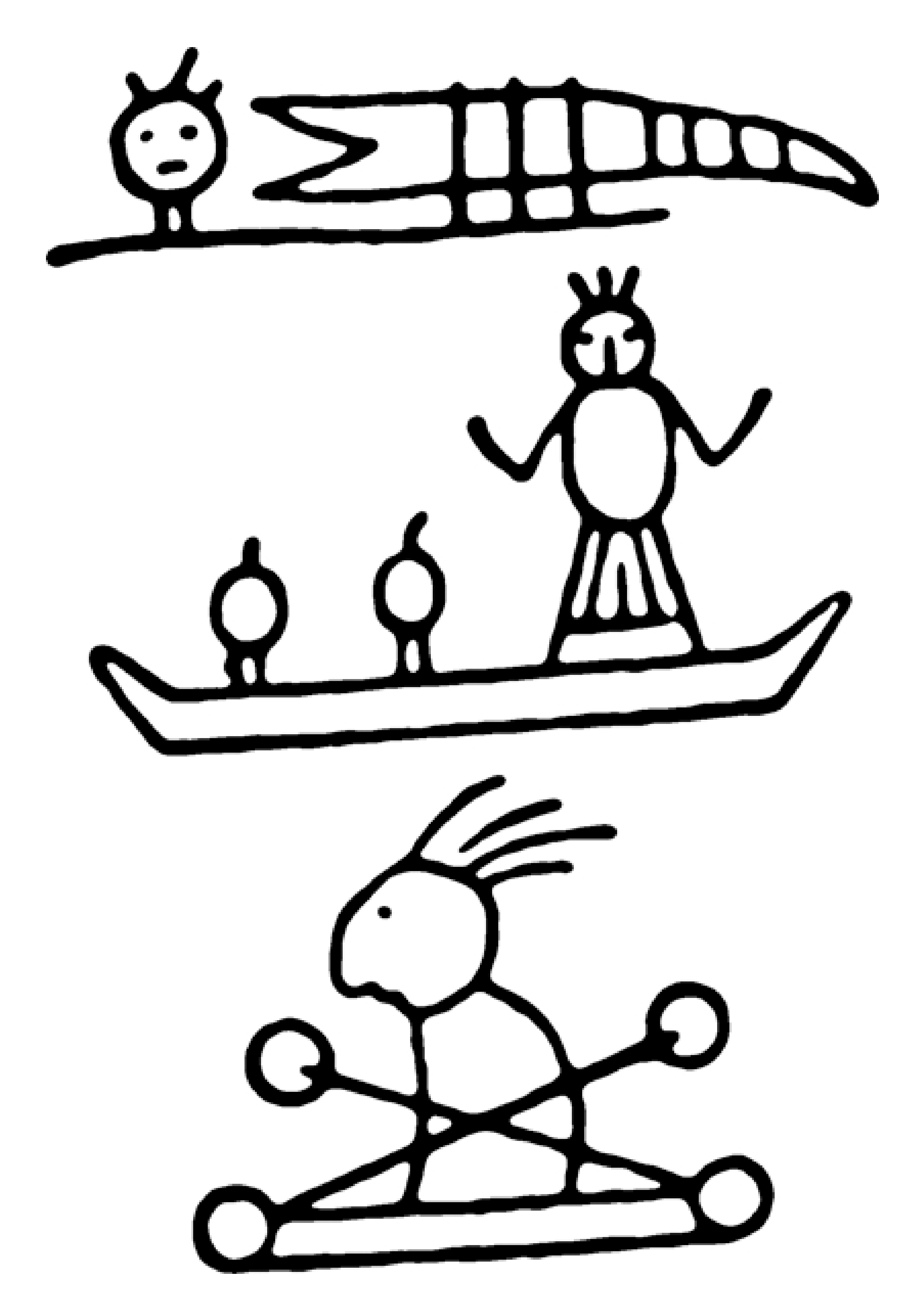
Мы же сейчас узнаем кое-что об истории письменности. Это полезно не только для общего развития, но и для того, чтобы у тебя как у криптоаналитика была информация о том, как различные народы кодируют свою речь при помощи письменных знаков. Так что готовься: я расскажу тебе очень много про разные алфавиты и системы письма, как они устроены и как их можно использовать для шифрования.

Но сначала я скажу тебе одну вещь. Мне в отрочестве приходилось доставать ту информацию, которую ты сейчас прочитаешь, по крупицам. Я собирал её по энциклопедиям и словарям, искал в справочниках по лингвистике, очень аккуратно перерисовывал в свои рабочие тетрадки. А ты сейчас получишь всё сразу (ну, не всё, а очень многое). В общем, впитывай эту информацию, она не только крайне интересна, но ещё и полезна во многих отношениях.

А теперь давай обратимся к истории письменности. Когда человек стал достаточно разумным для того, чтобы ему понадобилась передача информации, он понял, что ему необходима какая-то система письменности. Она позволила бы передавать информацию как в пространстве (то есть от одного человека другому), так и во времени (то есть работать как внешняя память). Но как записать то, что можно сказать?

Люди начали с того, что попытались рисовать смысл сообщения. Так возникло *пиктографическое письмо*. Оно было не очень приспособлено для передачи смысла, поскольку основывалось на изображении (по возможности реалистичном). Если человек хотел сказать «голова», то он рисовал голову, если «рука» – то руку. Ну и так далее. Ты, конечно, уже догадываешься об основной проблеме этого способа письма. Как, к примеру, передать понятие «разговаривать»? А более сложные и абстрактные понятия? Например, как написать слово «наука»? (Впрочем, тогда люди наукой не занимались, им это слово было совсем ни к чему).

Итак, в пиктографическом письме используются картинки – пиктограммы, которые как бы олицетворяют сообщаемое понятие. Обычно пиктограммы передают прямой смысл изображаемых рисунков (значков). Что-то более абстрактное передать при помощи пиктограмм затруднительно. Вот так примерно выглядит пиктографическое письмо:



Попробуй-ка разобраться – что имел в виду автор, рисуя эти знаки… Думаю, он и сам через несколько дней уже не помнил бы, что в точности хотел передать, какой смысл он вкладывал в эти изображения.

И тогда умные люди додумались использовать значки для передачи абстрактных смыслов. Это был существенный шаг вперёд по сравнению с простыми рисунками. Такая система письменности называется *идеографическое письмо*. Ее знаки, или идеограммы, получили расширенное толкование и стали обозначать уже не только тот объект, который нарисован,

но и многочисленные связанные с ним смыслы. Сами знаки постепенно стали более простыми и стандартизованными.

Идеографическая система письма интересна тем, что основной смысл знаков могут понять даже люди, не знающие языка, который записан идеограммами. Более того, иногда можно понять общий смысл надписи, совершенно не владея языком ее автора. Например, древнеегипетская идеограмма «волна» рисуется в виде волнистой линии, и это понятно без разъяснений любому человеку. Вот примеры нескольких идеограмм:



На представленном рисунке показаны прямые смыслы идеограмм: что нарисовано, то и обозначается. Но суть идеограмм в том, что они могут передавать и переносные значения. Так, к примеру, идеограмма «Чаша» может обозначать и понятие «пить».

Дальше развитие письменности пошло в двух направлениях. Из идеографического письма выделилось письмо иероглифическое. В нем идеограммы очень сильно упростились и даже стали более абстрактными. Впрочем, понятие «иероглиф» скорее бытовое, чем научное: обычно мы обозначаем этим словом какие-то непонятные значки. Например, китайская письменность традиционно называется «иероглифами», хотя каждый значок обозначает один слог, а не понятие. А в японском языке используются как иероглифы китайского языка, так и знаки слогового письма, которые уж никак не могут быть иероглифами (о слоговом письме мы поговорим ниже). Но в быту мы, как и подавляющее большинство людей, все равно называем иероглифами все японские знаки.

К примеру, вот немного китайских иероглифов:

В китайском языке много тысяч иероглифов, и уровень грамотности владеющего китайским определяется в том числе и количеством знаков, которые он знает. Есть и такая особенность – большинство использующих диалекты китайского языка могут не понимать друг друга, если они разговаривают, но написанное по-китайски понятно им всем. Японцы с корейцами тоже в целом поймут письменный китайский язык, хотя могут не понимать устный. Другими словами, китайское иероглифическое письмо переняло ту особенность идеографического письма, которую мы обсуждали выше.

Другими иероглифическими письменностями считаются египетское письмо (древнее), все клинописные системы письма и некоторые современные системы письма у африканских народов.

Второе направление, развившееся из идеографического письма, – это *алфавитное письмо*. Его мы хорошо знаем.

Надо сказать, что алфавиты не всегда были такими, какими мы знаем их сегодня. Они прошли долгий путь. Все началось с финикийского письма. Оно было одной из первых именно алфавитных систем, в которых каждый знак обозначал звук, а не слог или понятие. Были и другие подобные системы письма, но до сегодняшнего дня дожили лишь «потомки» финикийского письма, а другие системы алфавитной письменности не сохранились. Так что почти все современные алфавитные системы – наследницы финикийского письма.

Вот так выглядели финикийские знаки:

Знак	Первоначальные значения	Название	Примерный аналог в русском языке	Какая буква русского алфавита произошла от этого знака
	Бык	алп	—	А
	Дом	бет	Б	В
	Верблюд	гамл	Г	Г
	Дверь	делт	Д	Д
	Выдох, молитва, окно	he	—	Е, Ё
	Гвоздь, крючок	ўаў	—	У
	Оружие	зен	З	З
	?	хет	Х	И, Й
	Солнце	тъет	Т	—
	Рука	йод	Й	—
	Ладонь	каф	К	К
	Палка погонщика быков	лемда	Л	Л
	Воды	мем	М	М
	Рыба, угорь, змея	нун	Н	Н
	Опора, столб	семка	КС	—
	Глаз	гейн	Г (как южнорусское)	О
	Рот	пей	П	П
	?	съаде	С	Ц, Ч
	?	коф	—	Ф
	Голова	рош	Р	Р
	Зуб	шин	Ш	Ш, Щ
	Крест, знак, пометка	таў	Т	Т

Как видно, тут 22 знака, и все обозначают согласные. Здесь нет гласных, хотя в дальнейшем от некоторых из этих знаков произошли буквы русского языка, обозначающие гласные. Но древние финикийцы записывали только согласные звуки. Эту особенность унаследовали многие алфавиты Ближнего Востока (например, в арабском и еврейском письме тоже записываются только согласные).

Раз уж речь зашла об алфавитах, где записываются только согласные звуки (кстати, такие алфавиты называются *консонантными*), то давай изучим две современных системы письма – арабскую и еврейскую.

В арабской письменности слова пишутся справа налево, и начертание букв зависит от местоположения буквы в слове. Поэтому непосвящённому кажется, что в этой системе письма очень много разных знаков, хотя их всего 28. Кроме того, используется несколько дополнительных значков для вспомогательных целей. А сами знаки выглядят так, что их можно удобно соединить в так называемую *арабскую вязь*. Вот таблица:

Знак				Название	Примерное соответствие
В конце слова	В середине слова	В начале слова	Отдельно стоящий		
ـا		ا		алиф	—
ـب	ـبـ	بـ	ب	ба	Б
ـت	ـتـ	تـ	ت	та	Т
ـث	ـثـ	ثـ	ث	са	—
ـج	ـجـ	جـ	ج	джим	ДЖ, Г
ـح	ـحـ	حـ	ح	ха	Х
ـخ	ـخـ	خـ	خ	ха	Х
ـد		د		даль	Д
ـذ		ذ		заль	—
ـر		ر		ра	Р
ـز		ز		зай	З
ـس	ـسـ	سـ	س	син	С
ـش	ـشـ	شـ	ش	шин	Ш
ـص	ـصـ	صـ	ص	сад	С
ـض	ـضـ	ضـ	ض	дад	Д
ـط	ـطـ	طـ	ط	та	Т
ـظ	ـظـ	ظـ	ظ	за	З
ـع	ـعـ	عـ	ع	айн	—
ـغ	ـغـ	غـ	غ	гайн	Г
ـف	ـفـ	فـ	ف	фа	Ф
ـق	ـقـ	قـ	ق	каф	К
ـك	ـكـ	كـ	ك	каф	К
ـل	ـلـ	لـ	ل	лям	ЛЬ
ـم	ـمـ	مـ	م	мим	М
ـن	ـنـ	نـ	ن	нун	Н
ـه	ـهـ	هـ	ه	ха	Х
ـو		و		вав	В
ـي	ـيـ	يـ	ي	йа	Й

Пусть тебя не смущают встречающиеся в таблице одинаковые названия букв и большое количество одинаковых примерных соответствий. В арабском языке (и других языках, использующих эту письменность) имеются звуки, которых нет в русском языке, и им вообще сложно подобрать какое-либо соответствие. Арабы, к примеру, различают несколько различных звуков, которые мы воспринимаем просто как «К».

Честно говоря, использовать эту систему письменности для передачи русских слов практически невозможно. Например, не получится передать букву «О», поскольку в литературном арабском языке нет этого звука. А краткие гласные звуки на письме вообще не обозначаются.

А теперь давай посмотрим на еврейское письмо. Это письмо, так же как финикийское и арабское, относится к группе семитских алфавитов и используется в одном из еврейских языков – иврите. Это также консонантное письмо: в нем имеются знаки только для согласных звуков. Вот таблица:

Знак	Название	Примерное соответствие
א	алеф	А, Е
ב	бет	Б, В
ג	гимел	Г
ד	далет	Д
ה	he	Г (как южнорусское)
ו	вав	В, О, У
ז	зайн	З
ח	хет	Х
ט	тет	Т
י	йод	И, Й
כ, ך	каф	К, Х
ל	ламед	Л
מ, ם	мем	М
נ, ן	нун	Н
ס	самех	С
ע	аин	А, Е
פ, ף	пе	П, Ф
צ, ץ	цади	Ц
ק	коф	К
ר	реш	Р
ש	шин	Ш, С
ת	тав	Т

Если ты обратишь внимание на имена букв, приведённые в этих трёх таблицах, то увидишь практически полное их соответствие. Это показывает, что все три системы письма – родственные. Из этого, кстати, следует, что еврейская письменная система также плохо предназначена для передачи русских слов (хотя можно попробовать). Стоит отметить, что еврейское письмо также записывается справа налево.

Но как же при помощи этих алфавитов записывать гласные? Для этого используется два способа. Долгие гласные записываются при помощи соответствующих согласных (алеф – А, йод – И, вав – У). Краткие гласные либо не записываются вовсе, либо для них используется так называемая *огласовка*: при помощи специальных значков над и под основными знаками алфавита указываются эти самые гласные. Правда, обычно это используется в других языках, поскольку арабский и иврит устроены так, что записывать краткие гласные в них не нужно. Но тема эта очень широкая и разносторонняя, и если она тебя заинтересовала, то рекомендую обратиться к более специализированным источникам, которые легко можно найти в Интернете.

Мы же двинемся дальше и изучим другие системы письменности…

Теперь давай обратимся к более привычным нам системам письма. Одна из самых древних в Европе систем, основанная на финикийском письме, – греческий алфавит. Древние греки позаимствовали у финикийцев их письмо, но оно было совершенно не приспособлено для греческого языка. Как я уже упоминал, сам строй семитских языков устроен так, что на

письме не выделяются краткие гласные звуки. А в греческом языке не так: в нём гласные звуки, независимо от их долготы, очень важны. Поэтому грекам пришлось дополнить и видоизменить алфавит, чтобы приспособить его к своему языку. И у них появились знаки, которые соответствуют только гласным звукам языка.

Знак	Название	Примерное соответствие
Α α	альфа	А
Β β	бета	Б / В
Γ γ	гамма	Г / Н / Й
Δ δ	дельта	Д
Ε ε	эпсилон	Э
Ζ ζ	дзета	ДЗ / З
Η η	эта	И
Θ θ	тэта	Т
Ι ι	иота	И
Κ κ	каппа	К
Λ λ	лямбда	Л
Μ μ	мю	М
Ν ν	ню	Н
Ξ ξ	кси	КС
Ο ο	омикрон	О
Π π	пи	П
Ρ ρ	ро	Р
Σ σ ς	сигма	С
Τ τ	тау	Т
Υ υ	ипсилон	И
Φ φ	фи	Ф
Χ χ	хи	Х
Ψ ψ	пси	ПС
Ω ω	омега	О

Кроме того, в греческом алфавите были архаичные буквы, которые встречались всего в нескольких древних словах. Их ты найдёшь в справочниках. Эти буквы называются дигамма, хета, сан, коппа, сампи и шо.

От греческого письма произошли хорошо известные тебе латинский алфавит и кириллица. Латинский алфавит мы здесь рассматривать не будем, ты и так его прекрасно знаешь (если не знаешь, рекомендую выучить). А вот кириллицу мы изучим в ее старинном варианте: поскольку сегодня в русском языке используется не тот алфавит, который был придуман в IX веке, а так называемое «русское гражданское письмо». Вместе с кириллицей мы изучим и глаголицу – ещё один славянский алфавит, который использовался на Балканском полуострове у южных славян. Кириллица и глаголица практически полностью взаимозаменяемы. Вот таблица:

Знак кириллицы	Знак глаголицы	Название	Соответствие в современном русском языке
а	Ⰰ	аз	А
б	Ⰱ	буки	Б

в	Ⰲ	веди	В
г	Ⰳ	глаголи	Г
д	Ⰴ	добро	Д
є	Ⰵ	есть	Е
ж	Ⰶ	живете	Ж
ѕ	Ⰷ	зело	ДЗ
ꙁ,з	Ⰸ	земля	З
и	Ⰹ	иже	И
і,ї	Ⰺ, Ⰻ	и	И
к	Ⰽ	како	К
л	Ⰾ	люди	Л
м	Ⰿ	мыслете	М
н	Ⱀ	наш	Н
о	Ⱁ	он	О
п	Ⱂ	покой	П

Кириллица	Глаголица	Название	Звук
р	Ⱃ	рцы	Р
с	Ⱄ	слово	С
т	Ⱅ	твердо	Т
ѹ, ꙋ	Ⱆ	ук	У
ф	Ⱇ	ферт	Ф
х	Ⱈ	хер	Х
ѡ	Ⱉ	омега	О
щ	Ⱋ	шта	Щ
ц, ц	Ⱌ	ци	Ц
ч, ч	Ⱍ	червь	Ч
ш	Ⱎ	ша	Ш
ъ	Ⱏ	ер	Ъ
ꙑ	ⰟⰋ	еры	Ы
ь	Ⱐ	ерь	Ь
ѣ	Ⱑ	ять	Е
ю	Ⱓ	йотированный ук	Ю
ꙗ		йотированный аз	Я
ѥ		йотированный есть	Е
ѧ	Ⱔ	юс малый	
ѫ	Ⱘ	юс большой	
ѩ	Ⱗ	йотированный юс малый	
ѭ	Ⱙ	йотированный юс большой	
ѯ		кси	КС
ѱ		пси	ПС
ѳ	Ⱚ	фита	Ф
ѵ	Ⱛ	ижица	И
ꙉ	Ⰼ	гервь	Г (как южнорусское)
ѿ	Ⱉ	от	ОТ

Ты вспоминаешь знаки глаголицы, расположенные во втором столбце? Если нет, обратись к нашим занятиям на первой неделе.

Теперь давай изучим опыт германских и скандинавских племён и народов. Общего мнения о происхождении германских алфавитов нет, но считается, что они, скорее всего, произошли от греческого и латинского алфавитов. Их символы называются *рунами*.

Руны – это алфавитные знаки, предназначенные не только для письма, но и для разных магических целей. Древние германцы использовали их для гадания и создания амулетов. Существует довольно много разных рунических алфавитов. Практически каждый народ приспосабливал общегерманский рунический строй под свой язык, вводя в него новые символы. Но все они имеют одну особенность. Поскольку руны часто вырезали на камнях и дереве, они имеют угловатую форму. В древнегерманских мифах это объясняется тем, что верховный бог Один увидел руны в ветках деревьев, упавших на землю.

Всё это очень интересно, но выходит за рамки этой книги. Если ты заинтересуешься, то сможешь изучить все эти вопросы по дополнительным источникам. Мы же рассмотрим основной рунический алфавит.

Руниче-ский знак	**Название**	**Перевод**	**Примерное соответ-ствие**
ᚠ	fehu	скот	Ф
ᚢ	уруз	зубр	У
ᚦ	турисаз	шип	Т
ᚨ	ансуз	бог	А
ᚱ	райдо	путь	Р
ᚲ	кеназ	факел	К
ᚷ	гебо	дар	Г
ᚹ	вуньо	победа	В
ᚺ	хагелаз	град	Х
ᚾ	наудиз	нужда	Н
ᛁ	иса	лёд	И
ᛃ	йера	урожай	Й
ᛇ	эйваз	тис	Е
ᛈ	перто	память	П

ᛉ	альгиз	лось	З
ᛊ	совило	солнце	С
ᛏ	тиваз	Тюр	Т
ᛒ	беркано	берёза	Б
ᛖ	эваз	лошадь	Э
ᛗ	манназ	человек	М
ᛚ	лагуз	озеро	Л
ᛜ	ингваз	Ингви	НГ
ᛞ	дагаз	день	Д
ᛟ	одала	наследие	О

Руны хороши тем, что их можно «связывать» друг с другом, при этом получаются довольно интересные знаки. Древние германцы пользовались этим свойством для одного из видов рунической тайнописи. Но связанные руны применялись также и для магических целей.

Хочу отметить, что изначально слово «руна» относилось только к германским знакам. Но позже сходные надписи угловатыми знаками были обнаружены в разных регионах мира, в первую очередь в Сибири. Эти знаки никак не связаны с германскими рунами, просто похожи по начертанию, поэтому их тоже назвали рунами. Рассмотрим и их.

Рунический знак	Примерное соответствие
𐰀	А
𐰃	И
𐰆	О
𐰇	У
𐰉, 𐰋	Б
𐰑, 𐰓	Д
𐰍, 𐰏	Г
𐰞, 𐰠	Л
𐰣, 𐰤	Н
𐰺, 𐰼	Р
𐰽, 𐰾	С
𐱃, 𐱅	Т
𐰖, 𐰘	Й

𐰚, 𐰜	к
𐰲	ч
𐰢	м
𐰯	п
𐱁	ш
𐰔	з
𐰭	нг
𐰱	ич, чи, ч
𐰶	ик, ки, к
𐰸, 𐰹	ок, ук, ко, ку, к
𐰨	нч
𐰪	нй
𐰡	лт
𐰦	нт
:	пробел

Это знаки так называемой орхоно-енисейской письменности, которая в древние времена использовалась для записи многих языков тюркской семьи. Впоследствии из неё вышли венгерские руны и, предположительно, болгарские руны. Слова в этой письменности записывались справа налево.

В языках тюркской семьи существует различение гласных по ряду (которого нет в русском языке). Поэтому многие согласные в этой таблице представлены двумя знаками: первый используется с гласными переднего ряда, а второй, соответственно, с гласными заднего ряда. Пусть это тебя пока не волнует: тема эта выходит за рамки книги по криптографии, поскольку относится к лингвистике, филологии и этнографии.

Но вернёмся к рунам. Древние германцы жили по соседству с ещё более древними кельтами. Есть гипотеза, что свои руны они переняли именно у кельтов, а не у римлян и греков. Эта гипотеза вполне разумна, если посмотреть на то, как записывали свои слова кельтские племена. Они использовали так называемое *огамическое письмо*. Давай ознакомимся и с ним:

Огамический знак	Название	Примерное соответствие
ᚁ	берёза	Б
ᚂ	трава	Л
ᚃ	ольха	Ф
ᚄ	ива	С
ᚅ	раздвоенная ветка	Н
ᚆ	страх	Х
ᚇ	дуб	Д
ᚈ	железо	Т
ᚉ	орешник	К
ᚊ	куст	К
ᚋ	шея	М
ᚌ	поле	Г
ᚍ	ранение	НГ
ᚎ	сера	С
ᚏ	красный	Р
ᚐ	вяз	А
ᚑ	ясень	О
ᚒ	земля	У
ᚓ	?	Э
ᚔ	тис	И
ᚕ	осина	ЭА
ᚖ	золото	ОИ
ᚗ	локоть	УИ
ᚘ	шип	ИО
ᚙ	раздвоенный орешник	АЭ

Огамические тексты записывались по линейкам: чертились длинные горизонтальные или вертикальные линии, на которые затем «нанизывались» эти символы. В представленной таблице все символы написаны в горизонтальном положении, но их можно использовать и в вертикальном, повернув на 90 градусов против часовой стрелки.

Теперь давай рассмотрим необычные алфавиты, которые сохранились у небольших древних народов. Речь идёт об армянском и грузинском письме. Начнём с армянского:

Буква	Название	Примерное соответствие
Ա ա	айб	А
Բ բ	бен	Б
Գ գ	гим	Г
Դ դ	да	Д
Ե ե	еч	Е
Զ զ	за	З
Է է	э	Э
Ը ը	этх	Э
Թ թ	тхо	ТХ
Ժ ժ	жэ	Ж
Ի ի	ини	И
Լ լ	лиун	Л
Խ խ	хэ	Х
Ծ ծ	тса	ТС
Կ կ	кен	К
Հ հ	hо	Г (как южнорусское)
Ձ ձ	дза	ДЗ
Ղ ղ	гхат	ГХ
Ճ ճ	тшэ	ТШ
Մ մ	мен	М
Յ յ	йи	Й
Ն ն	ну	Н
Շ շ	ша	Ш
Ո ո	во	О, ВО
Չ չ	ча	Ч
Պ պ	пэ	П
Ջ ջ	джэ	ДЖ
Ռ ռ	рра	РР
Ս ս	сэ	С
Վ վ	веу	В
Տ տ	тиун	Т
Ր ր	рэ	Р
Ց ց	цо	Ц
Ւ ւ	hуун	У
Փ փ	пхиур	ПХ
Ք ք	кхэ	КХ
Օ օ	о	О
Ֆ ֆ	фэ	Ф

Грузинская письменность немного похожа на армянскую:

Буква	Название	Примерное соответствие
ა	ани	А
ბ	бани	Б
გ	гани	Г
დ	дони	Д
ე	эни	Э, Е
ვ	вини	В
ზ	зени	З
ჱ	—	—
თ	тани	Т
ი	ини	И
კ	кани	Н
ლ	ласи	Л
მ	мани	М
ნ	нари	Н
ჲ	хье	Й
ო	они	О
პ	пари	П
ჟ	жани	Ж
რ	раэ	Р
ს	сани	С
ტ	тари	Т
ჳ	вив	—
უ	уни	У
ფ	пхари	ПХ
ქ	кхани	КХ
ღ	гхани	ГХ
ყ	кари	К
შ	шини	Ш
ჩ	чини	Ч
ც	цани	Ц
ძ	дзили	ДЗ
წ	цили	Ц
ჭ	чари	Ч
ხ	хани	Х
ჴ	—	—
ჯ	джани	ДЖ
ჰ	хаэ	Х
ჵ	—	—

Эти системы письменности примечательны тем, что полностью отражают язык, в котором были созданы, и используются до сих пор. Поговаривают, что они были изобретены одним и тем же человеком (в чём я сомневаюсь).

Наконец, обратимся к азиатским системам письменности. В Азии их очень много, и если все перечислять, то не хватит места. Я уже упоминал о китайских иероглифах, когда мы изучали иероглифические системы письма. Но большая часть азиатских языков использует алфавитные системы письма. Просто на взгляд европейца эти алфавиты выглядят настолько необычно, что все эти знаки, значки и значочки в Европе называют «иероглифами», хоть это и неверно.

Давай изучим алфавит *деванагари*. Это индийский алфавит, который применяется в большинстве индийских языков, в том числе и в санскрите. Деванагари – *силлабическое письмо*, то есть в нём каждый знак обозначает слог, а не букву. Необходимо отметить, что в индийских языках так много непривычных для нашего слуха звуков, что очень сложно найти соответствие этих знакам в русском языке. Я постараюсь это сделать, но это будет неточным аналогом.

Согласные				
क КА	ख КХА	ग ГА	घ ГХА	ङ НГА
च ЦА	छ ЦХА	ज ЙА	झ ЙХА	ञ НЬА
ट ТА	ठ ТХА	ड ДА	ढ ДХА	ढ НА
त ТА	थ ТХА	द ДА	ध ДХА	न НА
प ПА	फ ПХА	ब БА	भ БХА	म МА
य ЙА	र РА	ल ЛА	व ВА	
श ЩА	ष ША	स СА	ह hA	
Гласные				
अ А	आ, ा АА	इ, ि И	ई, ी ИИ	उ, ु У
ऊ, ू УУ	ऋ ृ Р	ॠ, ॄ РР	ऌ ॢ Л	ॡ ॣ ЛЛ
ए, े Э	ऐ, ै АЙ	ऑ, ॉ О	ओ, ो ОО	औ, ौ АУ

Есть ещё несколько знаков, использующиеся в специальных случаях. Также есть знаки для согласных, которые присутствуют только в отдельных языках. Например, вот отдельные согласные для хинди, одного из официальных языков современной Индии:

क़ КА	ख़ КХА	ग़ ГА	ज़ ЗА	य़ ЖА	ड़ РА	ढ़ РХА	फ़ ФА

Как видишь, каждый знак в алфавите деванагари уже содержит гласный звук «А». Если есть необходимость написать согласный без гласного, то необходимо к знаку соответствующего слога добавить специальный значок: ् (в других языках этого рода этот подстрочный значок может отличаться). Пунктирный кружок здесь и в таблице для гласных обозначает символ согласного. Так что всё просто. Хотим из «КА» получить «КО» – пишем: को. И так далее…

Чтобы писать при помощи этого алфавита, необходимо сначала нарисовать горизонтальную линейку (как и для огамического письма), а потом на неё как бы «нанизывать» буквы-слоги.

В Азии существует ещё много алфавитов, начертанием отчасти похожих на деванагари. Есть бирманское письмо, есть тайское письмо, есть тамильское письмо и ещё множество подобных письменностей. С другой стороны, есть монгольское письмо и корейское письмо, которые тоже не так просты и употребляются только для записи соответствующих языков. В общем, привести все это множество письменностей в книге затруднительно. Но ещё пару алфавитов имеет смысл рассмотреть.

Давай изучим два японских алфавита. В японском языке используется три системы письменности. Одна называется «кандзи» и представляет собой просто китайские иероглифы, которые, однако, в японском языке читаются по-японски (на самом деле это не

совсем так, но в подробности мы сейчас вдаваться не будем). Обычно это корни слов. Две другие системы письма – это хирагана и катакана. Обе представляют собой слоговые письменности, в которых каждый знак обозначает один слог.

Начнём с хираганы. Эта система письма предназначена для записи японских слов. Обычно этой азбукой передают те слова, для записи которых нет иероглифа кандзи, а также для частицы, суффиксы и тому подобное. Также её можно употреблять вместо кандзи, если предполагается, что читатель может не знать каких-то иероглифов либо эти иероглифы незнакомы самому автору. Тексты, полностью записанные хираганой, обычно нужны для обучения детей-дошкольников. В таких текстах также используются пробелы между словами. Вот таблица:

	А	И	У	Э	О	Я	Ю	Ё
	あ	い	う	え	お	ゃ	ゅ	ょ
К	か	き	く	け	こ	きゃ	きゅ	きょ
С	さ	し	す	せ	そ	しゃ	しゅ	しょ
Т	た	ち	つ	て	と	ちゃ	ちゅ	ちょ
Н	な	に	ぬ	ね	の	にゃ	にゅ	にょ
Х	は	ひ	ふ	へ	ほ	ひゃ	ひゅ	ひょ
М	ま	み	む	め	も	みゃ	みゅ	みょ
Й	や		ゆ		よ			
Р	ら	り	る	れ	ろ	りゃ	りゅ	りょ
В	わ	ゐ		ゑ	を			
					ん			
Г	が	ぎ	ぐ	げ	ご	ぎゃ	ぎゅ	ぎょ
ДЗ	ざ	じ	ず	ぜ	ぞ	じゃ	じゅ	じょ
Д	だ	ぢ	づ	で	ど	ぢゃ	ぢゅ	ぢょ
Б	ば	び	ぶ	べ	ぼ	びゃ	びゅ	びょ
П	ぱ	ぴ	ぷ	ぺ	ぽ	ぴゃ	ぴゅ	ぴょ

В употреблении этих знаков есть свои особенности, и для их понимания необходимо учить японский язык. Мы этим сейчас заниматься не будем. Достаточно лишь сказать, что символ на пересечении строки и столбца читается как слог, составленный из согласной, которой обозначена строка, и гласной, которой обозначен столбец.

Вторая азбука – катакана – представляет собой тот же набор символов, только он используется для иных целей. Во-первых, при помощи катаканы записываются слова, заимствованные из тех языков, в которых не используются китайские иероглифы.
Во-вторых, она применяется для записи имён, звукоподражательных слов и всяких научных, технических и прочих специальных терминов.

	А	И	У	Э	О	Я	Ю	Ё
	ア	イ	ウ	エ	オ	ャ	ュ	ョ
К	カ	キ	ク	ケ	コ	キャ	キュ	キョ
С	サ	シ	ス	セ	ソ	シャ	シュ	ショ
Т	タ	チ	ツ	テ	ト	チャ	チュ	チョ
Н	ナ	ニ	ヌ	ネ	ノ	ニャ	ニュ	ニョ
Х	ハ	ヒ	フ	ヘ	ホ	ヒャ	ヒュ	ヒョ
М	マ	ミ	ム	メ	モ	ミャ	ミュ	ミョ
Й	ヤ	𛄠	ユ	イェ	ヨ			
Р	ラ	リ	ル	レ	ロ	リャ	リュ	リョ
В	ワ	ヰ	𛄢	ヱ	ヲ			
					ン			
Г	ガ	ギ	グ	ゲ	ゴ	ギャ	ギュ	ギョ
ДЗ	ザ	ジ	ズ	ゼ	ゾ	ジャ	ジュ	ジョ
Д	ダ	ヂ	ヅ	デ	ド	ヂャ	ヂュ	ヂョ
Б	バ	ビ	ブ	ベ	ボ	ビャ	ビュ	ビョ
П	パ	ピ	プ	ペ	ポ	ピャ	ピュ	ピョ
В	ヷ	ヸ	ヴ	ヹ	ヺ	ヴャ	ヴュ	ヴョ
Ц	ツァ	ツィ		ツェ	ツォ			
Ф	ファ	フィ	ホゥ	フェ	フォ	フャ	フュ	フョ

Как видно, набор символов здесь больше Это потому, что в исконном японском языке нет соответствий для некоторых согласных, которые присутствуют в заимствованных словах. Я не стал вносить в эту таблицу некоторые несущественные и редко используемые знаки. Всё это ты, если заинтересуешься, сможешь найти в специальной литературе.

Люди придумали и другие алфавиты – так называемые искусственные алфавиты для искусственных языков. Самый известный из них – алфавит *тенгвар*, который был разработан профессором Дж. Толкином для одного из придуманных им искусственных языков своего выдуманного мира. Другие искусственные алфавиты использовались для мистификаций. Например, существует книга под названием «Codex Seraphinianus». Это богато иллюстрированная книга, написанная на неизвестном языке неизвестным алфавитом. Лингвистический анализ показывает, что это действительно какой-то язык, а не случайный набор символов. Автор не раскрывает смысла написанного, а остальным до сих пор не удалось расшифровать её. Но еще более знаменита *рукопись Войнича*, которая была составлена в Средние века, но до сих пор люди даже и приблизиться не смогли к её расшифровке. Скорее всего, это тоже мистификация.

Наконец, среди искусственных алфавитов необходимо упомянуть алфавит философского языка *ифкуиль*, который настолько сложен, что те, кто говорят на нём, должны потратить длительное время, чтобы выразить самые простые фразы. Письменность его настолько же сложна, насколько и сам этот язык.

Все эти вскользь затронутые темы ты сможешь самостоятельно изучить при помощи дополнительных источников, в первую очередь, Интернета.

На этом мы закончим краткое введение в различные системы письменности и алфавиты.

Для чего мы всё это изучили? Всё просто. Во-первых, теперь ты сможешь распознавать знаки и, соответственно, языки, которыми, предположительно, записаны те или иные тексты. Во-вторых, теперь у тебя появился огромный набор разных символов, которые можно использовать в работе. Так что время от времени возвращайся к этой главе, а ещё лучше – заведи специальный альбом или картотеку, куда выписывай все встречающиеся тебе образцы письменности.

Неделя 8. Шифрование на основе редкой книги

Уф-ф-ф. Это было непросто. Столько новой информации удалось получить за прошлую неделю, не правда ли? Но теперь ты можешь отличать одни алфавиты от других, умеешь распознавать различные языки и при желании сможешь более интересно зашифровывать свои тайны. Ведь ты теперь знаешь, чем отличаются знаки-буквы от знаков-слогов.

Но всё это слишком просто. Давай постепенно переходить к шифрам, которые обладают очень мощной защитой от взлома. Как ты уже знаешь, все эти одноалфавитные и многоалфавитные замены никого не остановят. Они будут препятствием только для несведущих людей, а грамотный криптоаналитик взломает такие шифры, даже не поперхнувшись. Даже если ты будешь обозначать слоги разными символами, это не спасёт, ведь как только накопится достаточный объём шифрограмм, в них будут обнаруживаться многочисленные закономерности. А чем больше закономерностей, тем проще криптоаналитику расшифровать секрет.

А теперь представь, что шифрограмма состоит из последовательности чисел, среди которых ни одно не повторяется дважды. Как такое расшифровать? К скрытой таким способом тайне и подступиться-то страшновато. Даже если мы при помощи этого метода напишем целую книгу большого объёма, горе-криптоаналитику ничего не останется, как кусать локти. У него ничего не получится. Он повертит эти числа и так, и эдак, но сопоставить им какой-то смысл будет практически невозможно.

«*Книгу*»… Обрати внимание на это слово в предыдущем абзаце. Оно должно натолкнуть тебя на размышления. Предлагаю тебе сейчас отложить этот текст и подумать, как можно использовать книгу для шифрования.

Итак, в результате размышлений тебе в голову должен был прийти, по крайней мере, один способ шифрования при помощи книги. Давай-ка попробуем проверить. Я приведу несколько способов, которые пришли в голову мне, и ты сможешь сравнить свои догадки с моими. Вдруг тебе удалось меня превзойти?

В книге напечатан текст, который состоит из предложений, слов и букв (и других знаков, но они нам сейчас не очень-то и интересны). Мы можем выбрать из книги эти объекты. Но предложения выбирать крайне непродуктивно, поскольку вряд ли в произвольной книге ты найдёшь именно то предложение, которое хочется тебе написать – только если оно уж слишком простое и обыденное.

Слова. Да, возможно. Слов в книге много, так что можно выбирать слова. Надо просто пересчитать все слова и каждому назначить его номер. Но может случиться, что ты не найдёшь в книге нужное слово. К тому же такой способ шифрования очень трудоёмкий: тебе, по сути, придётся выучить наизусть текст из книги, чтобы помнить, где какое слово находится.

Буквы. Мы с тобой уже знаем, что буква – это минимальная графическая единица информации. Буквы не передают смысл, но их можно использовать для создания единиц более высокого уровня (то есть слов), которые смысл уже передают. Так что проще всего воспользоваться для шифрования буквами. Соответственно, на буквы надо как-то указывать, то есть необходима **система индексации.**

Что такое «система индексации»? Можно сказать, что это способ, который поможет нам понять, какую букву необходимо взять из книги. На ум сразу же приходит несколько таких способов:

1. Пересчитать все буквы в книге, дав им последовательно номера (*индексы*) от 1 и так далее до самой последней буквы. Это очень неудобный способ, поскольку числа будут всё увеличиваться и, в конце концов, достигнут астрономических размеров.

2. Можно указывать номер буквы на странице – а страницы в книгах уже пронумерованы. Тогда код для буквы будет состоять из двух чисел: номер страницы + номер буквы на странице. Этот способ намного легче, тем более что один из индексов уже создан (номера страниц).

3. Наконец, можно указывать номер страницы, номер строки на странице и номер буквы в строке. Уже три числа для каждой буквы! Но такой тройной индекс намного проще. И опять один из номеров уже напечатан в самой книге, остаётся найти два других.

В книге среднего объёма имеются сотни тысяч букв, так что для шифрования любой буквы ты сможешь использовать уникальный, ни разу не повторяющийся код. Нужно только помечать в книге те буквы, которые уже были использованы.

Как же шифровать таким методом? Необходимо выбрать в качестве ключа достаточно редкую книгу. По одному экземпляру такой книги должно быть у тебя и у того, с кем ты переписываешься. Итак, если ты хочешь зашифровать, скажем, слово «ПОБЕДА», то в произвольном месте книги ты должен найти букву «П» и записать её тройной индекс. Например, вот так: (20 17 35), что обозначает «буква на странице 20, в строке 17, на позиции 35». Шифрограмма всего слова будет примерно такой: (20 17 35) (6 5 3) (37 5 15) (32 5 21) (1 4 6) (5 13 7). Можно даже отказаться от скобок, поскольку довольно просто откладывать каждый раз по три числа и использовать их в качестве кода. Зато у криптоаналитика будет такая головная боль, что он спать не сможет! Если не использовать скобки, то начнут встречаться повторные числа, но это не должно тебя волновать: ведь это только затуманит и усложнит процесс расшифровки, и горе-криптоаналитик потратит огромное количество времени на частотный анализ, а он здесь вообще бессмыслен.

Соответственно, расшифровка происходит абсолютно так же, только в обратном направлении. Если тебе встречается код (20 17 35), то открой двадцатую страницу своей кодовой книги, отсчитай сверху семнадцатую строку, а в этой строке отсчитай тридцать пятую букву и выпиши ее. И так далее, для всей шифровки.

Этот метод шифрования практически невозможно взломать. Только благодаря удаче криптоаналитику в руки может попасть книга-ключ. Но при этом криптоаналитик должен еще и догадаться, что использовался описанный способ шифрования. В истории случались эпизоды, когда зашифрованные таким образом тексты были расшифрованы. Но это происходило только когда в качестве ключа была выбрана какая-то очень известная книга, а криптоаналитик знал, что шифрограмма зашифрована именно этим способом, и начинал просто перебирать все доступные ему книги. В конце концов шифрограмма поддавалась. Потому я напоминаю, что надо использовать редкую книгу либо вообще написать для этих целей уникальный текст.

Впрочем, иногда такие шифрограммы удаётся взломать и по-другому. Никто не отменял выкрадывание ключей, разные шпионские штучки и прочие не совсем честные методы. Поэтому храни свои криптографические ключи очень тщательно и оберегай их от чужого взгляда.

Теперь ты можешь приступать к выполнению задания. В письме, которое тебе придёт, будет шифрограмма, закодированная одним из описанных здесь способов. Попробуй применить к ней книгу из тех, что ты взял с собой.

Неделя 9. Замена целых понятий

На этой неделе мы изучим новую технику криптографии и шифрования. Она также позволяет очень хорошо защищать тайны и передавать оперативные сообщения. Эта техника основана на использовании кодовых слов.

Давай чётко разграничим понятия «*шифр*» и «*код*». Под шифром мы будем понимать (так понимают это все шифровальщики и криптоаналитики в мире) способ сокрытия информации путем замены или перемешивания единиц текста, которые не передают смысл (например, букв и слогов). В шифре также одновременно могут быть замена и перемешивание, в этом нет ничего удивительного. А термин «код» означает сокрытие информации на любом уровне, в том числе и на уровне единиц текста, обладающих смыслом. То есть кодировать можно и слова, и целые предложения, и даже целые тексты. Но кодировать можно и отдельные буквы. Так что любой шифр является кодом, но не каждый код будет шифром.

Теперь вспомни то, что я говорил ещё на первой неделе о простом шифре замены. Одноалфавитный шифр замены не является шифром, это просто код, в котором по-другому обозначаются буквы. Такие коды не слишком защищённые, их просто разгадать. Кстати, часто коды вообще не скрывают информацию, а используются для сокращения. Например, ты можешь выписать в столбик под номерами наименования всех своих книг. Номера и будут кодом, который можно использовать для сокращения. Вместо того чтобы писать или говорить, например, «Путешествие к центру Земли», можно будет использовать номер: 243.

Такие кодирующие списки еще называются *номенклаторы*. Номенклатор представляет собой простой словарь, в котором каждому кодовому слову соответствует какой-то специальный смысл. Соответственно, номенклаторы можно использовать в качестве ключей для кодирования информации.

Сам по себе этот метод шифрования выглядит не очень привлекательным. Он может быть вполне надёжным, но этому мешает несколько причин:

1. Хороший номенклатор должен содержать замены для тысяч слов, в том числе имён существительных, имён прилагательных и особенно глаголов. Только такой номенклатор позволит достаточно затуманить смысл передаваемых сообщений. Замена всего лишь нескольких ключевых понятий не слишком повысит надёжность кода, поскольку об их значении можно догадаться из контекста, особенно если они повторяются.

2. Если составить действительно большой номенклатор, окажется, что это просто новый язык, который использует ту же самую грамматическую основу, что и «материнский» язык, но заменяет корни слов на коды. Что ж, это тоже неплохой вариант. Во время Второй мировой войны так делали, но использовался очень редкий и очень сложный язык (язык индейского племени навахо), так что у криптоаналитиков не было никаких шансов.

3. Как всегда встаёт проблема секретного обмена ключами (то есть, в этом случае, номенклаторами) и тайного хранения этих ключей. Чем больше книга со словарём, тем сложнее уберечь её в секрете, и криптоаналитик сможет задействовать грубые методы: шпионаж, кражу или ещё что похуже. Так не раз бывало в истории.

Один из видов подобного кодирования – создание специализированного жаргона. Этим способом пользуются группы людей, которые хотят засекретить свои переговоры. В первую очередь (но не всегда) это преступные сообщества и религиозные секты.

Например, попытайся понять, о чём говорится в следующем тексте:

– *Мас скудается, устрекою шуры не прикосали бы и не отъюхтили бы шивару.*

– Так масы поёрчим бендюхом, а не меркутью. И шивару пулим ласо, а возомки забазлаем щавами. Не скудайся!

Это старинный кодовый язык торговцев-коробейников, или, как они сами себя называли, офеней. Многие слова из этого их кода потом стали называться *феней*, жаргоном преступного мира. По приведённому отрывку видно, что офени пользовались грамматикой русского языка, но заменяли все корни. Часто для этого брали корни из других языков: языков финно-угорских народов, (по землям которых ходили офени), цыганского языка и других. Перевод этого отрывка таков:

«*– Я боюсь, дорогою воры не побили бы и не отняли бы товару. – Так мы поедем днём, а не ночью. И товару купим мало, а повозки завяжем верёвками. Не бойся!*»

Итак, полагаю, что у тебя должна быть кодовая книга, полученная от того, кто занимается с тобой криптографией и посылает тебе письма. Если это так, то в очередном письме ты найдёшь новую шифрограмму, в которой используются коды из кодовой книги. Теперь ты знаешь, зачем это нужно и как это использовать. Можешь расшифровать послание и написать в ответ что-нибудь своё.

Если же кодовой книги у тебя нет, то теперь ты можешь составить её самостоятельно. Ты можешь привлечь к этой игре своих друзей, и у вас, возможно, получится собственный своеобразный язык. Попробуй…

Неделя 10. Симпатические чернила

На этой неделе мы изучим новый метод сокрытия информации, то есть стеганографии.

Представь себе чернила, написанное которыми невидимо в обычных условиях, но проявляется после применения определённых средств. Такие чернила называются *симпатическими*. Мы научимся делать разные виды симпатических чернил и проявлять то, что ими написано. Конечно же, мы узнаем и о том, как обнаруживать сообщения, написанные такими чернилами.

Начнём со способов, которые позволяют найти записи симпатическими чернилами. Предположим, тебе в руки (неважно, каким способом) попало письмо, отправленное незадачливым разбойником кому-то из своих подельников в обычном конверте. Твоя задача – узнать, что хотел передать разбойник. Ты открываешь конверт и видишь там чистый лист бумаги. Что ты думаешь? Правильно – на этом листе запись симпатическими чернилами. Разбойник поступил глупо. Чтобы его секрет не сразу открыли, не надо было отправлять пустой лист. Поверх тайной записи надо было написать какой-нибудь нейтральный текст обычными чернилами.

Допустим, разбойник оказался поумнее и как раз написал всякую ничего не значащую ерунду. Например, весь лист исписал рассказом о том, как он провёл прошлое лето в деревне у дедушки. В этом случае тебе надо проделать несколько проверок.

Сначала поверти письмо в руках так, чтобы свет на него падал под разными углами. Если ты вдруг заметишь блёстки, то тут точно использовались симпатические чернила. Блестят мелкие кристаллы вещества, использованного в качестве чернил.

Если блёсток нет, то надо внимательно рассмотреть под увеличительным стеклом структуру бумаги. Если структура нарушена, то есть волокна бумаги как-то изменяются, то дело явно нечисто.

Наконец, проще всего обнаружить надпись симпатическими чернилами, если нагреть лист бумаги. Очень многие (но не все) чернила проявляются при нагревании, так что можно обнаружить послание и сразу его прочитать.

Если нагрев не помог, то остаётся поместить лист бумаги в ультрафиолетовый свет: некоторые чернила видны в нём. Если и это не помогло, остается два варианта: либо разбойник использовал какие-то совсем необычные чернила, либо он действительно послал своим подельникам письмо про то, как он провёл лето, и никаких записей симпатическими чернилами на листе нет (но это не значит, что не применён другой метод сокрытия информации).

Какие же вещества можно применять в качестве симпатических чернил? О, таких веществ очень много. Посмотри внимательно на эту таблицу:

Чернила	**Проявитель**
Молоко	Нагрев
Яблочный сок	Нагрев
Сок лука	Нагрев
Сок брюквы	Нагрев
Свежая светлая моча	Нагрев
Квасцы	Нагрев
Спиртовой раствор пирамидона	Нагрев
Стиральный порошок с оптическим отбеливателем	Ультрафиолетовый свет
Воск	Мел или зубной порошок
Слюна	Очень слабый водный раствор чернил
Пищевая лимонная кислота	Бензиловый оранжевый индикатор
Крахмал	Йодная настойка
Аспирин	Соли железа
Фенолфталеин	Разбавленная щёлочь

Я попытался перечислить чернила и проявители для них, начиная с самых доступных. Самый простой проявитель – нагрев, а самые простые для нагрева симпатические чернила – молоко. Ну и все остальные пары в этой таблице расположены подобным образом.

Проще всего использовать именно молоко, но написанные им тайные послания легко обнаружить даже без нагрева бумаги. Ты можешь попробовать написать молоком что-либо на чистом листе, потом дождаться, когда оно высохнет, а затем внимательно рассмотреть лист. При определённых углах наклона будут видны отблески, особенно если бумага гладкая. Но если при этом скрыть тайные письмена под текстом, записанным обычными чернилами, то этот эффект будет смазан. Поэтому я рекомендую тебе всегда сначала писать тайный текст, а потом покрывать исписанный лист маскировочным текстом. И желательно использовать пористую, а не гладкую бумагу.

Думаю, что тебе будет очень интересно использовать в качестве симпатических чернил стиральный порошок с оптическим отбеливателем. Попробуй найти такой, растворить его в воде (столько, сколько растворится), а потом написать этой жидкостью тайный текст. Когда буквы высохнут, их снова можно будет увидеть только под ультрафиолетовым светом. Для этого требуется специальная лампа.

Теперь ты можешь приступать к решению загадки этой недели, которую тебе пришлет тот, с кем ты переписываешься. Когда ты решишь её, ты сможешь в ответ послать свою загадку. Попробуй в ответе использовать другие симпатические чернила.

Неделя 11. Каскадное шифрование

Наше обучение науке шифрования и сокрытия секретов почти закончено. К этому моменту ты уже знаешь очень и очень многое. Перед тем как перейти к главной теме – абсолютно невзламываемому шифру, – давай вспомним, что мы изучили. Итак:

1. Ты знаешь, что такое шифр одноалфавитной замены, как его взламывать, и понимаешь, что никогда нельзя скрывать свои секреты таким шифром, поскольку он абсолютно ненадёжен.

2. Ты умеешь использовать шифры многоалфавитной замены, умеешь отличать тексты, зашифрованные одноалфавитным шифром и многоалфавитным шифром (помнишь гистограммы частотности?). Ты знаешь, как взламывать многоалфавитные шифры при помощи вычисления длины ключа.

3. Ты можешь использовать метод стеганографии, который был предложен Фрэнсисом Бэконом в давние времена. Для этого используются разные характеристики символов текста, среди букв которого скрывается секретное сообщение.

4. Также ты в курсе нескольких специальных способов шифрования, вроде тарабарской грамоты, перестановочных шифров посредством решётки (дырявой матрицы, решётки Кардано) и кодирования целых понятий.

5. Ты знаешь о практически невзламываемом методе шифрования на основе редкой книги.

6. Наконец, на прошлой неделе мы изучили симпатические чернила, которые используются в качестве метода стеганографии для физического сокрытия секретного текста.

Всё это просто прекрасно. И перед тем как перейти к абсолютно невзламываемому шифру, я научу тебя ещё одному методу, который называется «*каскадное шифрование*». Его суть очень проста – просто-напросто используется несколько методов сокрытия информации, причём это могут быть и методы криптографии, и методы стеганографии.

Итак, мы берём текст, который необходимо скрыть, и применяем к нему какой-нибудь метод шифрования. Пусть, например, это будет шифр многоалфавитной замены с достаточно длинным ключом (не менее 10 символов, а лучше больше). Затем полученная шифрограмма скрывается ещё раз (только бессмысленно снова применять одноалфавитную или многоалфавитную замену – это не повысит уровень защиты). Например, шифрограмму можно перемешать при помощи дырявой матрицы. На третьем шаге мы можем закодировать полученную перестановку стеганографичным кодом Бэкона. И наконец, результат можно записать симпатическими чернилами, поверх которых написать какую-нибудь банальную и никому не интересную ерунду.

Представь себе работу криптоаналитика, который будет пытаться это расшифровать…

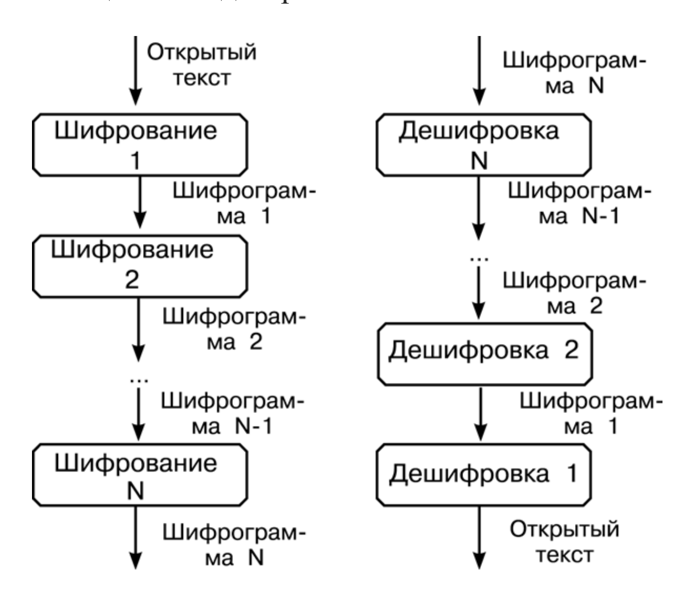
Давай рассмотрим пример. Скажем, какой-то хитрец перехватил послание, зашифрованное именно таким способом, как описано выше. Этот некто внимательно изучил лист с ничего не значащим текстом и обнаружил изменение структуры бумажных волокон. Он догадался, что на этом листе есть запись симпатическими чернилами. Он попробовал сначала ультрафиолетовое излучение, а потом нагрев бумаги, и на листе проявились буквы. Написан

какой-то текст, но буквы – то заглавные, то строчные вразнобой, и это дает намёк на то, что использован код Ф. Бэкона, то есть написанное симпатическими чернилами сообщение – тоже «обманка». Тогда этот проницательный человек декодирует код и получает последовательность букв. Построив гистограмму частотности разных букв, он понимает, что использован шифр многоалфавитной замены, поскольку гистограмма не соответствует русскому языку (также он проверил английский, немецкий и ещё несколько широко используемых языков; это не помогло). Тогда этот криптоаналитик пытается подобрать длину ключа, но не может найти в тексте повторов, потому что все буквы перемешаны. Много дней он ломает голову и приходит к выводу, что послание взломать невозможно. Впрочем, ему может улыбнуться удача, и он взломает шифр. Но это произойдёт, например, через год… А через год полученная из шифрограммы информация будет уже давно неактуальна.

Словом, суть каскадного шифрования заключается в том, чтобы при помощи достаточно простых способов настолько запутать и усложнить шифровку, что криптоаналитику, пусть даже он и знает об использованных методах, придется разгадывать все ключи и пароли очень долго. Так что к моменту, когда он закончит, информация безвозвратно устареет.

Понятно, что расшифровка послания, которое скрыто при помощи каскадного шифра, представляет собой обратный процесс. То есть если применялось три способа шифрования один за другим, то, расшифровывая, нужно будет применить эти же три способа, но в обратном порядке. Это важно, поскольку результат шифрования не сохраняется при перемене мест. Порядок всегда важен в шифровании.

Это можно пояснить при помощи такой диаграммы:



Для правильного использования каскадного шифрования нужно знать несколько базовых правил:

1. Одноалфавитный и многоалфавитный шифры замены – это один и тот же способ шифрования, поэтому их совместное использование бесполезно. Сколько бы разных ключей разной длины мы ни использовали для шифрования, всё это в итоге становится многоалфавитным шифром, который легко взламывается.

2. То же самое относится к перестановочным шифрам. Нет никакого резона использовать несколько разных ключей для перестановки букв в сообщении, потому что в итоге это будет выглядеть как одна перестановка.

3. Использование практически невзламываемых шифров для каскадного шифрования нецелесообразно, поскольку такие шифры очень долго разгадываются, даже если есть ключ. А смысл каскадного шифрования – в быстроте использования одновременно с катастрофическим увеличением времени взлома. Практически невзламываемые шифры, типа шифра на основе редкой книги, сами по себе практически бесконечно затрудняют работу криптоаналитика.

4. Лучше всего сначала применить несколько методов криптографии, а потом скрыть послание при помощи одного или нескольких методов стеганографии.

Теперь ты знаешь об этой теме всё, что требуется для успешного использования каскадного шифрования и, главное, для расшифровки. На этой неделе ты получишь письмо, в котором шифровка составлена с использованием каскада шифров и методов стеганографии. Так что у тебя есть все возможности для того, чтобы продемонстрировать в деле полученные за лето умения.

Неделя 12. Одноразовый блокнот

Наконец, мы приступаем к изучению системы шифрования, которая не может быть взломана, если ею правильно пользоваться. Это вершина криптографической мысли. При этом сам шифр настолько прост, что можно только удивляться тому, почему эта система не используется везде и всеми. Впрочем, далее я разъясню тебе, почему её сложно использовать, и она не нашла широкого применения. Получается, что сам шифр простой, а вот использовать его сложно. Парадокс.

Но начнём. Вспомни, пожалуйста, тему четвёртой недели, когда мы изучали новую математическую операцию XOR. Сейчас это тебе пригодится. Если требуется, перечитай соответствующую главу и выполни несколько упражнений, применяя операцию XOR к двоичным числам. А теперь продолжай чтение.

Представь, что тебе необходимо зашифровать какую-либо фразу. Пусть это будет простое слово «КАТАПУЛЬТА». В качестве ключа для применения операции XOR пусть используется последовательность символов «ВОАЫДЛАОВЬ». Что получится в результате? Правильно: последовательность «ЗНСЭФЧМУПЩ», которая и будет нашей шифрограммой.

Если криптоаналитик перехватит шифрограмму, у него окажется этот странный текст: «ЗНСЭФЧМУПЩ». Как подойти к расшифровке? Он может последовательно перебирать все возможные ключи, в какой-то момент наткнётся на ключ «АЕРЪГЯКЩШЫ» и при расшифровке получит слово «ИЗВЕРЖЕНИЕ». Дальше он встретит ключ «АКУСРИЛШЭЪ», которому при расшифровке будет соответствовать слово «ИДЕОГРАММА». И так далее.

Очевидно, что так криптоаналитик переберёт все возможные ключи и получит все возможные слова длиной в 10 букв (даже больше, он получит и обрывки фраз длиной в 10 букв). Но какое из них верное? Нет никакой возможности выбрать правильный вариант, поскольку ни один ключ не будет правильным словом – все ключи окажутся случайными наборами символов.

Это описание рассказывает о сути невзламываемой системе шифрования. Вот она вся как есть:

1. Для шифрования текста необходимо воспользоваться операцией XOR.

2. Ключ должен быть такой же длины, как и шифруемый открытый текст.

3. Ключ должен состоять из случайного набора символов.

4. Ни один ключ не должен использоваться более одного раза. Никогда! Ни при каких условиях!

Эти четыре простых правила дают абсолютную защиту.

Давай подробнее разберём, что происходит и почему необходимо неукоснительно соблюдать эти правила, чтобы шифр невозможно было взломать.

Правило первое на самом деле не такое уж абсолютное. Дело в том, что, как мы уже видели, операция XOR даёт очень простой и быстрый способ получения из двух букв новой. Но точно так же можно воспользоваться и любой другой таблицей подстановки – например, той, что приведена в описании второй недели, то есть шифром сдвига. Да и вообще можно составить любую таблицу многоалфавитной замены, где способ замены будет определяться буквой ключа. Главное, чтобы она была удобна и однозначна. Мне кажется удобной именно таблица для операции XOR.

Второе правило говорит о том, что длина ключа должна быть равна длине шифруемого сообщения. Это просто объяснить. Если длина ключа будет меньше длины шифруемого сообщения, то ключ будет повторяться при шифровании. А как взламывать шифрограммы с периодическим ключом, мы уже изучили на второй неделе. Да, если ключ будет достаточно длинным, взломать сообщение будет сложно. Но *возможно*.

Третье правило: ключ должен быть абсолютно случаен. Нельзя использовать в качестве ключа какой-либо осмысленный текст. Это было понятно из описания попыток горе-аналитика взломать шифрограмму слова «КАТАПУЛЬТА». Если бы это слово было зашифровано при помощи другого осмысленного слова, то в процессе перебора криптоаналитик наткнулся бы на такой осмысленный ключ и сделал резонный вывод, что он получил расшифровку. Кроме того, если использовать осмысленный ключ (даже и такой же длины, как и шифруемое сообщение), тайное послание превратится в банальный шифр многоалфавитной замены, к которому применим частотный анализ. Более того, не придется задумываться о длине ключа, поскольку надо будет анализировать частоты пар символов.

Наконец, главное правило: никогда, ни при каких условиях один и тот же ключ нельзя использовать дважды. Это очень важно. Всё дело в том, что если криптоаналитик получит два сообщения, зашифрованные одним и тем же ключом, каким бы длинным он ни был, то оба этих сообщения будут очень быстро взломаны. Можно просто применить к ним обоим операцию XOR, и тогда, насколько ты помнишь её свойства, секретный ключ просто взаимоуничтожится, и получится зашифрованное сообщение, состоящее из двух осмысленных текстов. А это очень легко взламывается частотным анализом. Дело тут даже не в операции XOR. Любая таблица многоалфавитной замены предполагает обратную операцию. Просто операция XOR обратна сама для себя, поэтому она так удобна.

Как происходит такое шифрование? У двух людей, которые желают обмениваться секретными данными этим абсолютно надёжным способом, должны быть специальные одинаковые блокноты с ключами. На каждой странице такого блокнота написаны случайные символы. Когда первый человек посылает второму секретное сообщение, он зашифровывает его при помощи ключа на первой странице блокнота. Второй человек, получив сообщение, расшифровывает его при помощи такого же ключа на первой странице его блокнота. После этого и первый и второй вырывают первую страницу блокнота и уничтожают её (лучше всего сжечь и смешать пепел; если просто выкинуть страницу с ключом в мусорное ведро, то она может быть найдена зловредным криптоаналитиком, и тогда всё пропало). Далее всё повторяется. Каждый раз после использования ключа с очередной страницы эта страница уничтожается. Потому-то метод и называется *одноразовым блокнотом*.

Теперь ты знаешь, как расшифровать ту шифрограмму, которая пришла в письме на этой неделе. Поищи, у тебя должен быть ключ, который передан тебе заранее.

Теперь я расскажу тебе, почему этот способ шифрования не используется так широко. Если ты подумаешь, то поймёшь, что проблема заключается в передаче ключа. Одноразовый ключ должен быть заранее создан и получен теми двумя лицами, которые должны обмениваться секретной информацией. Это сделать не так сложно, если их действительно всего двое. А представь, к примеру, штаб, которому необходимо обмениваться секретной информацией с сотнями разведчиков по всему миру. Одноразовые блокноты не должны повторяться у разных людей. То есть для каждого разведчика надо создать свой блокнот, как-то передать его, а потом время от времени обновлять, когда блокнот заканчивается. Это связано с очень большими расходами и риском раскрыть свою агентурную сеть.

Передавать же секретный ключ по открытым каналам связи, как ты понимаешь, нельзя. Это должна быть надёжная передача, а пока не придумали ничего надёжнее, чем передача из рук в руки. Впрочем, существует метод скрытой передачи по открытому каналу. Но он связан с серьёзной математикой, и его описание выходит за рамки этой книги. К тому же он всё равно остаётся довольно громоздким и проблематичным. Так что мы изучим его в другой раз. Но и этот метод полностью не решает проблемы *распределения ключей* (запомни, кстати, этот термин).

Но возможно, ты можешь передать секретные ключи одному или нескольким своим коллегам по секретной переписке. Тогда я сейчас научу тебя генерировать такие ключи. И ты поймёшь, что это тоже непросто и связано с большим расходом времени и сил.

Вспомни, как мы научились кодировать все буквы алфавита при помощи пяти двоичных цифр (нулей и единиц). Для каждой буквы нужно пять двоичных цифр, то есть пять бит информации. Как получить случайные пять бит? Да очень просто. Для этого надо воспользоваться пятью монетками. Возьми пять монет разного достоинства (чтобы различать их): 10 копеек, 50 копеек, 1 рубль, 2 рубля и 5 рублей (или какие-то еще). Орёл обозначает 0, решка обозначает 1. Брось пять монет и запиши результат по порядку от 10 копеек до 5 рублей. Таким способом ты получишь один символ. Если все монеты выпадут орлом (это соответствует 00000, то есть пробел), то не используй этот символ.

Таким способом ты сможешь сгенерировать ключ произвольной длины. Его надо записать в двух экземплярах, один оставить у себя, а второй передать тому, с кем ты собираешься вести секретную переписку. Конечно, твой друг должен быть обучен методу использования одноразового блокнота.

На этом наше путешествие в мир криптографии и криптоаналитики заканчивается. Но я затрону ещё две интересные темы, которые останутся тебе в качестве домашнего задания (про них не будет знать тот, с кем ты переписывался всё лето). А в самом конце книги я перечислю, что интересного можно почитать на тему криптографии, если ты заинтересовался этой областью прикладной науки.

Домашнее задание 1. Шифр подстановки для пар символов

Вот тебе первое домашнее задание. Придумай шифр «одноалфавитной» подстановки, но не как обычно, для каждой буквы, а по одному символу для пары букв. Возьми уже знакомый алфавит из тридцати двух символов и составь таблицу размером 32 × 32. Строки и столбцы таблицы обозначь символами нашего алфавита. А в каждой ячейке придумай замену паре символов в виде какого-нибудь экзотического знака.

Использовать такой шифр будет просто. Весь открытый текст разбивается на пары символов. Например, пусть надо зашифровать текст «СЕГОДНЯ Я ДОДЕЛАЮ ЭТО ДЕЛО». Разбиение на пары символов происходит следующим образом:
«СЕ-ГО-ДН-Я_-Я_-ДО-ДЕ-ЛА-Ю_-ЭТ-О_-ДЕ-ЛО». Каждой паре символов соответствует один символ замены из твоей таблицы.

Выбирать символ замены надо по строке и столбцу. Первая буква в паре соответствует столбцу, а вторая – строке. Соответственно, в шифрограмме будет в два раза меньше символов, чем в открытом тексте, а разнообразие символов будет больше.

Всего в твоей таблице будет 1024 ячейки, которые надо заполнить. Но подумай, все ли ячейки стоит заполнять. Какие комбинации букв в русском языке отсутствуют? После того как ты сделаешь эту таблицу и потренируешься шифровать свои сообщения с её помощью, рекомендую тебе поразмышлять над тем, как взломать этот шифр. Это не так сложно, как кажется на первый взгляд. Свои идеи можешь присылать мне для проверки и обсуждения на адрес электронной почты: *roman.dushkin@gmail.com*.

Когда-то давным-давно, после того как я обучил своих одноклассников методу частотного анализа, и для них перестало быть секретом то, как я взламывал их секретные послания, я составил для себя такую таблицу и писал свои секретные сообщения при помощи шифра подстановки для пар символов. Это, конечно же, снова привело к тому, что никто не мог взломать мои шифровки. Более того, никто даже не мог понять, что за шифр я использую. Так-то…

Домашнее задание 2. Дисковая машина для шифрования

Теперь я предлагаю тебе сделать механическое устройство для очень стойкого шифрования. Это будет практически одноразовый блокнот – если этим устройством пользоваться правильно и никогда не нарушать установленные принципы. Такое устройство для шифрования было создано в Германии между мировыми войнами и известно под кодовым названием «Энигма». Это была довольно компактная для тех времён электромеханическая машина, которая позволяла шифровать сообщения при помощи очень стойкого шифра. И только безалаберность немцев, допускавших ошибки и погрешности при её использовании, а также немного везения позволили полякам и затем англичанам взломать её.

Мы не будем делать полную копию немецкой «Энигмы», поскольку это не слишком-то просто. Я опишу тебе принцип действия и дам чертежи простой бумажной версии. Ты сможешь сделать облегчённую модель, которой будет вполне достаточно для твоих нужд. Но, зная принципы, заложенные в эту машину, ты сможешь создать и более серьёзную модель. Так что давай с ней ознакомимся.

Я не буду рассказывать про то, как устроена немецкая шифровальная машина «Энигма», а лучше в списке литературы дам ссылки на книги, в которых это прекрасно описывается. Вместо этого сразу обратимся к принципам, на которых «Энигма» (и та машина, которую мы сделаем) работает. Вот они:

1. Использование машины представляет собой применение шифра простой одноалфавитной замены.

2. Машина состоит из нескольких *роторов*, то есть вращающихся дисков, каждый из которых представляет собой шифр одноалфавитной замены.

3. Нюанс заключается в том, что этот шифр меняется для каждой следующей буквы текста.

4. Количество таких различных шифров одноалфавитной замены можно сделать астрономически большим, так что в идеальном случае повторов не будет никогда, а потому это будет равносильно использованию одноразового блокнота.

5. У машины можно выбирать так называемое *начальное состояние*, которое определяет то, как роторы расположены относительно друг друга.

6. Также у машины есть *отражатель*, который позволяет сделать так, что шифрование и расшифровка производятся одним и тем же способом.

У настоящих роторных шифровальных машин есть ещё некоторые способы усложнения их шифров, но в нашей «маленькой» версии мы обойдёмся только несколькими роторами и отражателем.

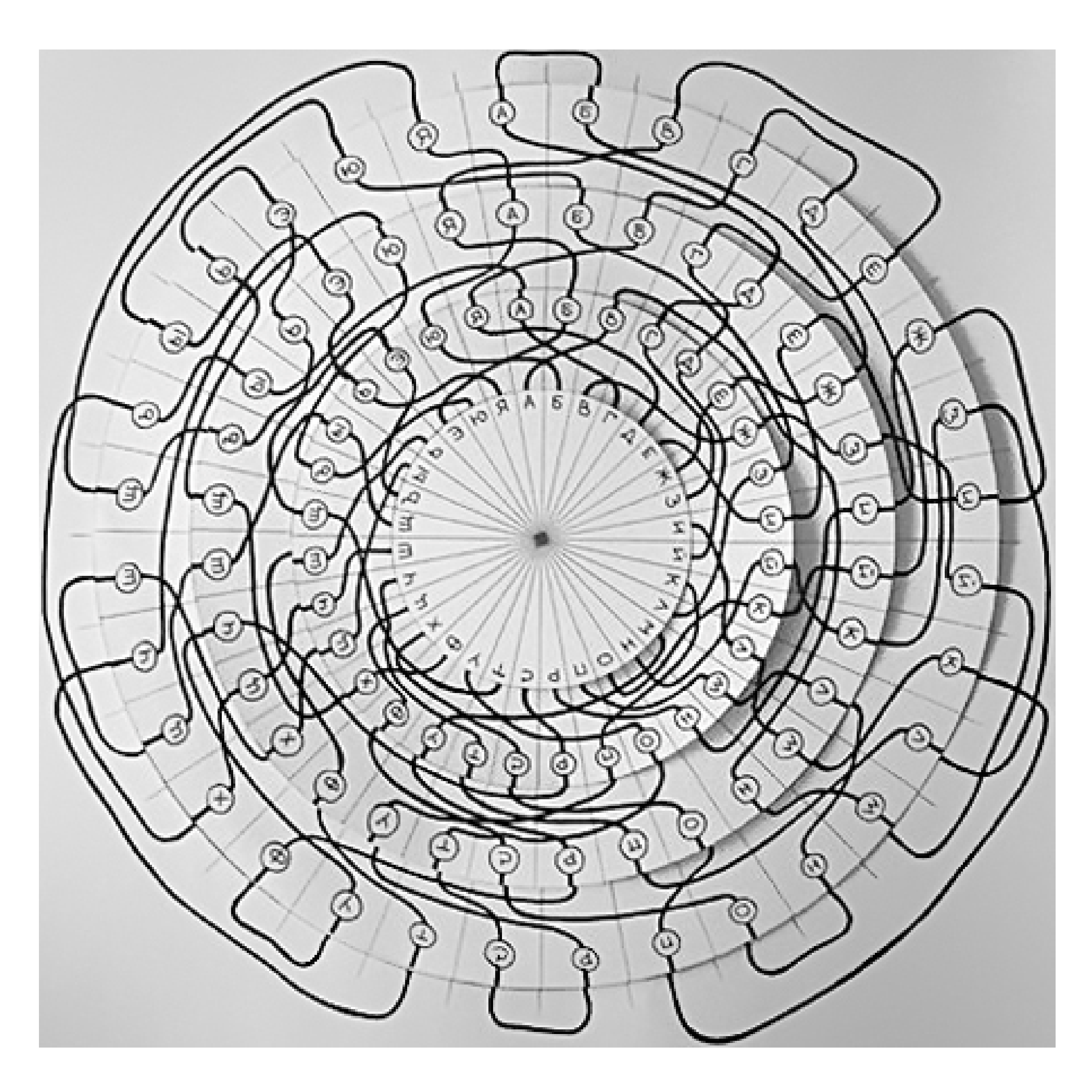
Теперь давай немного изменим правила игры. Всё лето мы в своих шифрограммах использовали пробел. Но ты уже знаешь, что пробел – это плохой для шифрования символ, поскольку он очень часто встречается. Слишком часто. Мы удалим этот символ из наших текстов, тем более что в подавляющем большинстве случаев текст без пробелов можно легко восстановить: тыжеможешьсделатьэто?

Итак, пробела у нас больше нет, но 32 символа в нашем алфавите нужно сохранить, поскольку, как ты помнишь, это круглое число в двоичной системе счисления. Теперь мы разделим буквы «Ъ» и «Ь», так что алфавит будет выглядеть так:

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Ничего нового и удивительного.

Но почему нам надо оставить 32 символа? Всё просто. Буквы мы нанесем на бумажные диски (которые будут аналогами роторов), а это означает, что диски надо будет разделить на столько секторов, сколько используется букв. Разделить диск на 32 сектора очень просто: надо разделить диск пополам, потом каждую половину ещё раз пополам, потом ещё, ещё и ещё раз, то есть всего пять раз. Итого окажется 32 сектора. (Вспомни двоичную систему счисления и то, почему число 32 в ней является круглым!).



Общий вид дисковой машины для шифрования, которую я научу тебя делать, таков:

На первый взгляд – это какое-то хаотичное переплетение непонятных линий. Но если ты немного присмотришься, то увидишь четыре бумажных диска, лежащие друг на друге, и все они находятся на подложке. Каждый диск разбит ровно на 32 сектора, и в каждом секторе написано по букве нашего нового алфавита. На изображении диски повернуты так, чтобы буквы в секторах на всех дисках находились ровно напротив друг друга. Жирные чёрные линии на рисунке показывают так называемую проводку. Это провода, идущие от буквы к букве через все диски. Наконец, лист, на котором лежат диски, представляет собой отражатель. Если ты приглядишься к нему, то поймёшь, почему он так называется. Всё просто: на отражателе все провода выходят из одной буквы, а входят в другую, то есть как бы отражаются.

Как шифровать при помощи этой машины? Алгоритм несложный. Например, тебе надо зашифровать букву «А». Ты ведёшь взглядом по линии, выходящей от буквы «А» на самом верхнем диске. На втором диске линия приходит к букве «В», далее на третьем диске к букве «Н» и на четвёртом диске к букве «М». Затем через отражатель провод возвращается к букве «Й» на четвёртом диске, затем идёт к букве «З» на третьем и «Ж» на втором диске, после

чего возвращается на первый диск на букву «В». Это и будет шифром для буквы «А». Так можно зашифровать любую букву алфавита.

Как ты понимаешь, это очень простой шифр одноалфавитной замены. Он тем более простой, что является симметричным (за счёт отражателя). То есть если буква «А» шифруется при помощи буквы «В», то буква «В» шифруется при помощи буквы «А». И так с любой парой букв.

Как же сделать так, чтобы шифр был стойким? Ведь понятно, что если шифровать так, как написано в предыдущем абзаце, то ни о какой стойкости говорить не приходится.

Всё просто. Всё настолько просто, что ты даже можешь придумать метод самостоятельно. Так что я рекомендую тебе подумать, прежде чем читать дальше. Обрати внимание на то, что диски могут вращаться относительно друг друга.

Итак, если твой метод основан на вращении дисков после шифрования каждой буквы, то твоя мысль верна. Всё действительно очень просто. Как только мы зашифровали букву, мы должны повернуть самый верхний диск на один сектор по часовой стрелке, и следующая буква будет шифроваться по совершенно иной проводке. Например, если во взаимном расположении дисков машины (для краткости будем называть это расположение «конфигурацией») на рисунке буква «А» шифровалась как «В», то при повороте верхнего диска на один сектор по часовой стрелке буква «А» станет шифроваться как «Щ». Если ещё раз так же повернуть верхний диск, то буква «А» будет шифроваться как «Ю». Таким образом, первоначальный текст «ААА» будет зашифрован как «ВЩЮ».

Но это не всё, конечно же. Ясно, что раз секторов на диске всего 32, то один диск позволяет использовать тридцать два алфавита замены. Если вращать только верхний диск, то фактически это будет использование шифра многоалфавитной замены с длиной ключа в 32 символа. Это достаточно много, но легко подлежит взлому, как ты уже знаешь из занятий второй недели. Поэтому нужны новые вращающиеся диски. Но они вращаются тогда, когда предыдущий диск делает полный оборот. То есть когда верхний диск делает полный оборот, второй диск поворачивается по часовой стрелке на один сектор.

Так тоже получается шифр многоалфавитной замены, но каждый новый диск умножает длину ключа на количество секторов на нём, то есть на 32. На представленной схеме четыре диска, а потому общая длина ключа, которым можно зашифровать послание, равняется 1048576. Представь себе: более миллиона символов, причём эти замены в основном случайны. Другими словами, для посланий, длина которых меньше миллиона букв, используется одноразовый блокнот (это не совсем так, но для простоты можно считать именно так, особенно если не нарушать правил шифрования).

Но и это ещё не всё. Если каждый раз начинать с одной и той же позиции взаимного расположения дисков, то ни к чему хорошему это не приведёт. Это всё равно как для одноразового блокнота дважды использовать один и тот же ключ. Но и тут спасает возможность вращения дисков. Мы же можем выставлять произвольную начальную конфигурацию, выбирая одну из миллиона. Мы можем каждый день выбирать новую конфигурацию, и этого хватит на всю жизнь. Начальная конфигурация определяется тем, какие буквы стоят друг напротив друга на дисках. Для этого на отражателе нужно выбрать начальный сектор, который лучше всего пометить стрелкой (на моём рисунке этого не сделано). Соответственно, начальная конфигурация зависит от того, какие буквы на дисках расположены напротив стрелки, начиная с верхнего диска. Можно, например, сказать, что начальная конфигурация на рисунке – «АААА», если стрелку на отражателе нарисовать напротив того сектора, где расположена буква «А» на самом нижнем диске.

Итак, правила шифрования:

1. Сначала надо выбрать и установить начальную конфигурацию дисков относительно друг друга. Проще всего каждый день выбирать новую конфигурацию. Правило определения начальных конфигураций для каждого дня должно быть известно всем, кто участвует в секретной переписке.

2. Затем надо выбрать ключ для тайного сообщения. Первые четыре буквы шифрограммы должны определять этот ключ, то есть конфигурацию дисков для текущего сообщения. После того как четыре буквы зашифрованы, диски переводятся в новое положение. Это сделано, чтобы для каждого сообщения в течение одного дня использовались разные ключи.

3. Таким образом, ключ дня используется в шифровке ключей для каждого конкретного сообщения, а сообщения шифруются при помощи своих индивидуальных ключей. Ключ в этом случае – просто взаимное расположение дисков. Если ты сделаешь машину, состоящую из другого количества дисков (это возможно), то, соответственно, количество первых букв сообщения, определяющих ключ, будет равно количеству дисков.

4. Затем для шифрования используется метод многоалфавитной замены, когда диски вращаются относительно друг друга при каждом новом выборе буквы.

5. После зашифровки сообщения машина возвращается в начальную конфигурацию, выбранную на этот день.

6. Чтобы расшифровать принятое сообщение, машину надо перевести в конфигурацию дня, после чего расшифровать первые четыре буквы. Это ключ сообщения. Машина должна быть установлена в новую конфигурацию. Как только это сделано, происходит расшифровка сообщения. Это делается абсолютно так же, как и шифрование, поскольку машина создает симметричный шифр замены.

7. Никогда не используй для ключей сообщений какие-то слова или повторяющиеся буквы. Каждый раз это должны быть случайные наборы букв. Чтобы получать такие наборы, пользуйся методом с пятью монетками, который был описан в главе об одноразовом блокноте.

Вот и всё. Рекомендую тебе обдумать написанное и сделать такую машину для своих секретных нужд. Ты вполне можешь использовать другой способ соединения проводки, а не перерисовывать схему выше. В приложении к этой книге ты найдёшь шаблоны для распечатки на бумаге и создания своей машины.

Дерзай!

Заключение

Вот и закончились наши приключения. Надеюсь, что тебе понравилось. Также очень надеюсь, что у тебя сложилось положительное мнение о криптографии и криптоаналитике, и теперь ты сможешь самостоятельно продолжать занятия в этой области. К тому же в процессе чтения книги тебе пришлось хорошо продвинуться в математике.

Если тебя увлекла эта область, то в следующем разделе я дам ссылки на другие книги по криптографии. Среди них ты сможешь выбрать то, что тебе наиболее интересно и подходит для дальнейшей работы.

Кроме всего прочего, ты всегда можешь написать мне письмо по адресу электронной почты: *roman.dushkin@gmail.com*, чтобы обсудить прочитанное, узнать, что делать дальше, и, если интересно, получить новые задачи и загадки.

Всего доброго!

Список литературы

Сначала несколько художественных книг, где рассказывается про то, как ловкие главные герои взломали шифры:

1. **Жюль Верн**. *Путешествие к центру Земли*. Довольно интересная книга автора многочисленных приключенческих и научно-фантастических романов XIX века, сюжет которой рассказывает о путешествии трёх отважных героев под землёй. Примечательна первая глава, в которой главный герой разгадывает зашифрованный манускрипт, ставший причиной их дальнейших приключений.

2. **Артур Конан Дойль**. *Пляшущие человечки*. Рассказ из цикла про Шерлока Холмса, частного детектива и просто прекрасного человека. Фабула рассказа заключается в расшифровывании Шерлоком Холмсом таинственных надписей, сделанных при помощи замысловатого шифра подстановки без пробелов. В рассказе описывается метод подбора ключевых слов.

3. **Эдгар По**. *Золотой жук*. Классическое произведение, вызвавшее увлечение криптографией и криптоаналитикой у обычных читателей. Автор досконально рассказывает о том, как взломать простой шифр одноалфавитной замены при помощи частотного анализа. Сюжет рассказа также примечателен: пираты, клады и так далее.

Теперь несколько научно-популярных книг:

4. **Дэвид Кан**. *Взломщики кодов*. Популяризаторская книга о криптографии, о том, как она начиналась, как развивалась, каких успехов достигла. Много рассказывается о том, как взламывались те или иные системы шифрования, в том числе и немецкая шифровальная машина «Энигма».

5. **Саймон Сингх.** *Книга шифров. Тайная история шифров и их расшифровки*. Занятная книга о криптографии, в которой приводится уйма интересных историй и познавательных описаний систем шифрования. Чтение несложное, книга популярная и простая.

6. **Роберт Чёрчхаус**. *Коды и шифры, Юлий Цезарь, «Энигма» и Интернет*. Ещё одна книга с историческими очерками о криптографии, как всё начиналось и куда пришло на современном этапе. Написана достаточно легко и вполне интересна.

Если же ты, прочитав эти книги, поймёшь, что хочешь продолжения, то напиши мне письмо на электронную почту, и я дам дальнейшие рекомендации.

Дополнение (для родителей)

Дорогие друзья!

«Математика и криптография» – это уникальное издание с методическими рекомендациями для изучения и практического использования методов шифрования. Книга поможет развить математические способности и логическое мышление. Кроме того, попытки создать собственные шифры раскрывают творческие способности ребенка. Игровой формат повествования позволит с легкостью удерживать внимание ребенка на протяжении всех занятий. Единственная пока в своем роде, книга откроет маленьким читателям еще одну грань самопознания и поможет определиться с выбором интересов и, возможно, будущей профессии.

Криптография – одна из старейших наук, и зародилась она более трех тысяч лет назад. Первоначально письменность сама по себе была криптографической системой, так как в

древних обществах ею владели только избранные. Сегодня вы получили возможность соприкоснуться с этой, ранее тайной, математической наукой в простом изложении для детей и взрослых.

Русская криптографическая школа и по сегодняшний день является одной из самых сильных в мире. Академией криптографии Российской Федерации ежегодно проводится межрегиональная олимпиада школьников по математике и криптографии, которая включена в перечень олимпиад школьников, утверждаемый Министерством образования и науки России, что позволяет предоставлять льготы победителям и призерам олимпиады при поступлении в ВУЗы. Ассоциация «РусКрипто», которой уже более 20 лет, поддерживает традиции развития отечественной криптографии, проводя ежегодные научные и практические конференции и семинары по криптографии. И книжка, которую вы держите в руках, одобрена экспертами для изучения детьми вместе с их родителями.

Желаем родителям и детям каждый день открывать новое, учиться друг у друга и главное – проводить больше времени вместе. А книга станет отличным поводом для этого.

Член Совета директоров Ассоциации «РусКрипто»

Юрий Малинин



Для взрослых детей – маленькая подсказка

Этот текст представляет собой двенадцать небольших занимательных заметок о **криптографии** – науке о шифровании и дешифровке (математических методах защиты информации). Он для родителей детей от 10 лет, которые хотели бы устроить для своих чад незабываемый отдых, наполненный тайнами и шпионскими штучками, а заодно подтянуть и развить их навыки в математике, информатике и программировании. В этой части книги приводятся методические рекомендации о том, как устроить досуг ребёнка во время летних каникул, так что каждая из двенадцати заметок соответствует одной неделе отдыха. Предполагается, что эту часть будет читать родитель, который должен будет незримо направлять ребёнка по пути изучения криптографии – и сам будет активно изучать эту науку.

Введение

Идея этой книги возникла у меня после лета 2014 года, когда я не смог приехать на дачу к старшему сыну, который проводил там все летние каникулы. Тогда, для того чтобы хоть как-то общаться с сыном и заниматься его развитием, я придумал метод обучения новым знаниям и тренировки полученных за учебный год навыков в области математики и русского языка. Не всё получилось так, как я задумывал, но эта методика позволила заинтересовать сына, научить его некоторым новым и интересным методам работы, а также провести в общении с ним незабываемые дни.

Теперь у меня возникла идея оформить наработанные материалы в виде двух книг: одна из них предназначена для родителя и содержит описание того, как заниматься с ребёнком, то есть как работать с темами, чтобы ребёнок был заинтересован. Вторая книга предназначена для детей, и в ней приводятся описания разных способов шифрования и взлома шифров так, чтобы было понятно вдумчивому ребёнку в возрасте старше десяти лет. Обе книги описывают одно и то же разными словами и в разных аспектах; книги синхронизированы, а потому читать их надо одновременно и параллельно.

Для чтения этой книги необходимо обладать математическими навыками, по крайней мере, понимать математику на уровне полной средней школы (а лучше – ещё лучше). Будет очень здорово, если читатель имеет навыки программирования, поскольку многие методы шифрования проще и удобнее применять при помощи специальной компьютерной программы. Хотя эта книга написана так, чтобы использование компьютера не было необходимым, всегда полезно потренироваться в реализации алгоритмов и написании программ. Тем не менее все описанные здесь занятия криптографией можно провести в «ручном режиме».

Конечно, математические навыки и дружба с математикой потребуются и ребёнку, с которым вам предстоит заниматься. Без них ему, скорее всего, будет просто непонятна, а следовательно, и неинтересна предлагаемая игра. Впрочем, знающий и понимающий родитель сможет переработать предлагаемые в книге методы в соответствии с характером и уровнем развития своего ребёнка.

Если у читателя несколько детей близкого возраста, с которыми можно устроить такие «шпионские игры», то эта книга также подойдёт. Можно устроить эту игру с каждым ребёнком отдельно, но это, скорее всего, вызовет непонимание у детей. Можно устроить соревнования, но тут также есть свои риски. Лучше всего, на мой взгляд, как-то объединить усилия детей, чтобы они одновременно решали задачи и отгадывали загадки. Надеюсь, что мои методические рекомендации помогут в этом.

В Интернете я планирую размещать дополнительные материалы для обучения ребёнка основам криптографии. Эти материалы помогут как с методологической точки зрения, так и для создания различных криптографических ресурсов: ключей, одноразовых блокнотов, шифров и кодов. Также я намереваюсь публиковать программы для использования и дальнейшей самостоятельной доработки, чтобы они были инструментами – как в деле обучения криптографии, так и в самих вопросах шифрования и дешифровки. В любом случае заинтересованный читатель всегда может написать мне на адрес электронной почты: *roman.dushkin@gmail.com*, и мы сможем обсудить практически каждый вопрос, касающийся этой книги.

В добрый путь!

Методические рекомендации

Прежде чем вы начнете со своим ребёнком игру, которая научит его основам криптографии, я хотел бы дать некоторые методические рекомендации. Они основаны на моём личном опыте, а потому их стоит воспринимать только лишь в качестве советов, но никак не догм. У меня нет педагогического образования, все мои наработки основаны только на опыте занятий со старшим сыном. Поэтому всякий читающий должен критически относиться к написанному и применять этот текст к своим конкретным условиям.

Обучение основам криптографии по этой книге рассчитано на 12 недель. Этот срок выбран как примерная длительность летних каникул. Соответственно, читателю, принявшему решение провести со своим ребёнком лето в изучении секретов криптографии, стоит заранее ознакомиться с этой книгой, чтобы быть готовым ко всем занятиям, а также примерно спланировать эту деятельность. Отдать же ребенку его книгу («Книга для детей») желательно уже на первой неделе занятий.

В детской книге, конечно же, написано, что ребёнок должен всё держать в тайне, в том числе и саму книгу. Однако я рекомендую взрослому также ознакомиться с ней заранее. Тем, у кого нет навыков криптографии и криптоанализа, она позволит понять, чем же вы будете заниматься с ребёнком всё лето. В любом случае это будет небезынтересно. И кроме того, советую тем из читателей, у кого нет знаний об этой науке, прочитать дополнительную литературу. Список рекомендуемых книг приведён в конце этого труда.

Основная идея обучения при помощи этих книг, заключается в отправке друг другу писем. Возможно, ребёнку будет сложно или неинтересно писать ответы, но взрослый должен каждую неделю посылать одно письмо, в котором раскрывается одна из тем. Так что в этой книге рассказывается, как готовить еженедельные послания, как зашифровывать или скрывать сообщения тем методом, которому посвящена неделя. А вот в книге для ребёнка объясняется, что это за письмо, какой метод шифрования был применён и как его можно взломать.

Вот основные рекомендации, как сделать процесс обучения интересным для ребёнка:

1. Писать письма лучше всего вручную, а не печатать на принтере. Если ребёнок читает ещё с трудом, то желательно использовать печатные буквы (да и вообще всегда лучше их использовать). Для писем подойдёт обычная писчая бумага формата А4. Лучше не использовать разлинованные листы. Если писать на пустом листе тяжело, то можно использовать разлинованную подложку. Это позволит сделать письмо опрятным (само собой разумеется, что помарок и исправлений лучше не допускать).

2. Конверты тоже лучше использовать самодельные или даже складывать письма «треугольниками», как во время Великой Отечественной войны.

3. Рекомендую придумать для этих писем какую-нибудь необычную особенность. К примеру, мы со старшим сыном переписывались, скрепляя письма настоящей сургучной печатью. Да, в специальном магазине был куплен сургуч и печать для него. Мы сворачивали письма в треугольный конверт (при этом добавляли дополнительный лист с распечатанной сеткой, чтобы невозможно было разглядеть написанное на просвет), треугольник оборачивали лентой и запечатывали сургучом и печатью. Это было не только аутентично, но и достаточно эстетично.

4. Необходимо продумать канал передачи писем. Если ребёнок живёт, к примеру, на даче с бабушкой и дедушкой, а еженедельно к нему кто-нибудь ездит, то письма можно передавать с этим посыльным. Если вы живёте вместе с ребёнком, то можно устроить специальный почтовый ящик, ключ от которого будет только у ребёнка, а взрослый сможет опускать

письмо через прорезь. Это придаст дополнительной таинственности – ребенок сможет забирать адресованные ему письма тогда, когда никто за ним не наблюдает.

5. Было бы неплохо время от времени спрашивать ребёнка о его успехах в криптографической теории и практике. Если у него появляются сложности, то с ребёнком надо дополнительно проработать тему и вопросы, которые вызвали эти затруднения. Это необходимо делать крайне осторожно и скрупулёзно, поскольку знания, предлагаемые в этой книге, действительно непросты, и при попытках взять их с наскока можно понизить ребёнку мотивацию.

6. Кроме того, для занятий на восьмой неделе ребёнку необходимо дать какую-либо книгу, в которой не жалко будет зачёркивать буквы. Другой экземпляр этой книги надо оставить у себя. Лучше всего заранее ознакомиться с материалами восьмой недели, чтобы подготовиться основательно.

7. Для занятий на девятой неделе необходимо составить словарь кодовых понятий и также передать один экземпляр ребёнку (в принципе, это можно сделать и во время занятий, но лучше составить заранее). Опять же советую ознакомиться с описанием задачи девятой недели прямо сейчас.

8. Наконец, для занятий на последней, двенадцатой неделе потребуется одноразовый блокнот, который надо составить, распечатать в двух экземплярах и один отдать юному криптографу. Прочитайте описание двенадцатой недели заранее.

Вот так, к примеру, выглядело треугольное письмо, которое я каждую неделю отправлял старшему сыну на дачу.



Надеюсь, что методические рекомендации помогут вам провести незабываемые часы и дни досуга одновременно с обучением непростой и крайне интересной теме.

Неделя 1. Простой шифр подстановки

На первой неделе юный криптограф будет изучать основополагающие понятия науки о шифрах. Для этого проще всего использовать шифр простой подстановки. Другими словами, в таком шифре все буквы заменяются на какие-либо другие символы (возможно даже, на те же самые буквы, только в измененном порядке). Соответственно, шифрограмма выглядит

как тот же самый текст, только в нём все буквы заменены на другие символы. Технически это вовсе не шифр, но для тех, кто незнаком с криптографией, даже такое будет разгадать не очень просто.

Вот, что потребуется для организации занятия:

1. Какое-либо сообщение длиной не менее 500 символов (не считая пробелов).

2. Шифр простой подстановки. Для этого необходимо сделать таблицу шириной в 33 столбца и высотой в две строки. В верхней строке пишутся все буквы русского алфавита, в нижней строке ставятся символы, которые эти буквы заменяют. Это ключ.

3. Текст из пункта 1, преобразованный в шифрограмму с использованием ключа из пункта 2. Чтобы преобразовать его, нужно заменить буквы текста на соответствующие значки ключа.

4. Письмо для ребёнка, в тексте которого приводится шифрограмма. В самом письме может быть указано всё что угодно. Например, можно написать про текущие дела, про погоду или планы на грядущие выходные, а где-нибудь в середине текста надо вставить шифрограмму.

Ребёнок, получив письмо, должен будет шифрограмму разгадать. Для того чтобы понять, что ребёнок справился с заданием, в самой шифрограмме нужно будет написать какое-то конкретное задание, которое ребёнок должен будет выполнить.

Давайте посмотрим, как это можно сделать. Пусть для шифрования заготовлен следующий текст:

ПРИВЕТ. Я РАД, ЧТО ТЫ СРАЗУ ЖЕ ДЕЛАЕШЬ УСПЕХИ В КРИПТОАНАЛИЗЕ И УЖЕ МОЖЕШЬ РАЗГАДЫВАТЬ ТАКИЕ ЗАДАЧИ, КАК ВЗЛОМ ШИФРА ПРОСТОЙ ПОДСТАНОВКИ. КАК ВИДИШЬ, ЭТО СОВСЕМ НЕСЛОЖНО, НАДО ТОЛЬКО ДОСТАТОЧНО ТЕРПЕНИЯ И УСИДЧИВОСТИ. И ТЕПЕРЬ ТЫ ПОНИМАЕШЬ, ЧТО ТАКИМ СПОСОБОМ ШИФРОВАНИЯ ПОЛЬЗОВАТЬСЯ ДЛЯ СОКРЫТИЯ СВОИХ СЕКРЕТОВ НЕЛЬЗЯ НИ В КОЕМ СЛУЧАЕ. ЛЮБОЙ ЧЕЛОВЕК, КТО МАЛО-МАЛЬСКИ ЗНАКОМ С МЕТОДОМ ДЕШИФРОВКИ ПО ЧАСТОТАМ, ВЗЛОМАЕТ ТАКОЙ ШИФР В ДВА СЧЁТА. ПРОДОЛЖАЙ ЗАНИМАТЬСЯ, И МЫ ИЗУЧИМ ЕЩЁ МНОГО ИНТЕРЕСНОГО. ПОКА.

Примечание: как видите, тут использованы только заглавные буквы. Обычно при шифровании и дешифровке используют только заглавные (или только строчные) буквы, поскольку для передачи смысла нет никакой разницы в том, заглавная буква в тексте или строчная. Если пытаться их различать в шифре, то это увеличит объёмы необходимых вычислений, но никак не увеличит сложность самого шифра.

Теперь сделаем какой-нибудь простой шифр подстановки с заковыристыми символами. Например, пусть код будет такой:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
α	β	ϐ	γ	δ	ε	η	ξ	ζ	ι	ϊ
К	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**
κ	λ	μ	ν	ω	π	ρ	σ	τ	υ	φ
Х	**Ц**	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**	**Ю**	**Я**
χ	ς	ψ	θ	ϕ	ϱ	Ϛ	Ƒ	ϡ	ϟ	ϒ

И теперь совсем несложно зашифровать текст:

πριϐετ. ϒ ραδ, ψτω τϛ σραζυ ξε δελαεθF υσπεχι ϐ κριπτωαναλιζε ι υξε μωξεθF ραζγαδϛϐατF τακιε ζαδαψι, κακ ϐζλωμ θιφρα πρωστωϊ πωδστανωϐκι. κακ ϐιδιθF, ϡτω σωϐσεμ νεσλωξνω, ναδω τωλFκω δωστατωψνω τερπενιϒ ι υσιδψιϐωστι. ι τεπερF τϛ πωνιμαεθF, ψτω τακιμ σπωσωϐωμ θιφρωϐανιϒ πωλFζωϐατFσϒ δλϒ σωκρϛτιϒ σϐωιχ σεκρετωϐ νελFζϒ νι ϐ κωεμ σλυψαε. λϟϐωϊ ψελωϐεκ, κτω μαλω-μαλFσκι ζνακωμ σ μετωδωμ δεθιφρωϐκι πω ψαστωταμ, ϐζλωμαετ τακωϊ θιφρ ϐ δϐα σψητα. πρωδωλξαϊ ζανιματFσϒ, ι μϛ ιζυψιμ εφη μνωγω ιντερεσνωγω. πωκα.

Честно говоря, конкретно в этом шифре фантазии немного. В качестве шифровальных символов использованы строчные знаки греческого алфавита, а для специфических русских букв, у которых нет соответствия в греческом языке, взяты редкие значки из древнегреческого языка или его диалектов. Тот, кто знает греческий алфавит, сможет прочитать эту шифрограмму и без ключа. Но пока в качестве примера подойдёт и такой вариант. Осталось посоветовать, что для первого занятия надо бы придумать что-то своё и интересное.

После того как текст закодирован и шифрограмма построена, её можно встраивать в письмо. Отправьте письмо ребёнку, понаблюдайте и зафиксируйте результат. Если у ребёнка возникли сложности с заданием, то ему следует помочь.

Неделя 2. Шифр многоалфавитной замены

В этой главе я предлагаю рассмотреть шифры многоалфавитной замены. Но перед этим имеет смысл договориться о том, что мы больше не будем использовать какие-либо особые значки, а всё будем шифровать при помощи тех же самых букв, какие используются и для записи открытого текста, то есть букв русского алфавита. В этом нет ничего удивительного или необычного: в криптографии только так всё и делается, поскольку, как стало ясно по результатам занятий на прошлой неделе, нет никакого резона использовать специальные знаки, ибо сами по себе они шифр не усложняют.

Что такое шифр многоалфавитной замены? Его суть заключается в том, что к открытому тексту применяется процедура шифрования, основанная на циклическом применении заданного ключа. Ключом в этом случае служит какое-либо кодовое слово. Чем длиннее слово, тем больше используется алфавитов для шифра.

Для шифрования применяется следующая процедура. Пробелу и каждой букве русского алфавита ставится в соответствие число от 0 до 31, причём 0 – это пробел, буква «А» имеет код 1, буква «Б» – код 2 и т. д. Договоримся, что буквы «Е» и «Ё» не различаются, а также не различаются буквы «Ъ» и «Ь» – причина всего этого будет ясна позже, главное, что теперь символов *ровно* 32 (это 2^5, поэтому для математика это число «круглое»). Хорошая новость заключается в том, что теперь коды букв можно складывать друг с другом. Сложив коды двух букв (открытого текста и ключа), получаем новую букву. Она-то и является буквой шифрограммы. Если в результате сложения получается код, больший 31, то от этого кода надо отнять 32 (в математике это представляет собой операцию сложения по модулю 32; да и вообще модульная арифметика, или арифметика остатков, очень часто нужна в деле криптографии).

Допустим, что в качестве ключа выбрано слово «БУКВА», тогда процедура шифрования выглядит следующим образом:

Открытый текст	Ключ	**Шифрограмма**
Ч	Б	Щ
Т	У	Ж
О	К	Щ
	В	В
Т	А	У
А	Б	В
К	У	Я
О	К	Щ
Е	В	И
	А	А
Ш	Б	Ъ
И	У	Э
Ф	К	
Р	В	У

Вот так при применении ключа к открытому тексту получилась шифрограмма: «ЩЖЩВУВЯЩИАЪЭ У». Среди 14 букв этой шифрограммы трижды встречается буква «Щ», и это уже должно вызвать подозрение, что не всё так просто. Этот шифр более стойкий, чем простая одноалфавитная замена, но всё ещё настолько простой для обученного криптоаналитика, что применять его бесполезно – он будет взломан мгновенно.

Для удобства и ускорения работы можно сделать таблицу размером 32 × 32 ячейки:

		А	**Б**	**В**	**…**
		А	Б	В	…
А	А	Б	В	Г	…
Б	Б	В	Г	Д	…
В	В	Г	Д	Е	…
…	…	…	…	…	…

По такой таблице сразу видно, что сложение букв «Б» и «В» даёт букву «Д» (ищем ячейку на пересечении «Б» и «В», причём неважно, в строке или в столбце стоят буквы, поскольку операция коммутативна) и т. д.

Теперь надо выполнить две несложные задачи:

1. Придумать сообщение, длина которого должна быть не менее 500 символов.

2. Придумать ключ длиной в четыре символа. Если ключ короче четырёх символов, то шифрограмму будет взломать очень просто, а более длинные ключи сделают работу юного криптоаналитика слишком сложной, и он, скорее всего, отставит эту задачу и это занятие как слишком утомительное. В целях обучения я крайне рекомендую в качестве ключа использовать какое-либо *слово*, знакомое ребёнку, а не случайное сочетание букв.

3. Зашифровать придуманное сообщение при помощи процедуры сложения с ключом.

Всё ранее описанное можно осуществить при помощи арифметики вычетов по модулю 32. Если каждому символу алфавита от пробела до буквы «Я» поставить в соответствие число от 0 до 31, то в совокупности с арифметическими операциями сложения и вычитания получится кольцо Z_{32}. Тогда шифрование будет представлено в этом кольце как сложение кодов символов открытого текста и ключа, а дешифровка как вычитание кодов символов ключа из символов шифрограммы соответственно.

Давайте попробуем сделать такую шифровку. Здесь не будет открытого текста длиной не менее 500 символов, используем более короткий. Пусть это будет текст: «ХОРОШО ТЕМ КТО НАУЧИЛСЯ ШИФРОВАТЬ СООБЩЕНИЯ ХОРОШО», а ключом пусть будет слово «ШИФР». Как видно, здесь не используются знаки препинания. В принципе, они никогда не используются при шифровании, поскольку избыточны.

Начнём: Х + Ш = О. О + И = Ч. Р + Ф = Е. О + Р = ПРОБЕЛ. Ну и так далее. В итоге получается шифрограмма: «**ОЧЕ СЧФГЯХФЫЛЧФЯЩЭМЩДЪУРССЙБЗЛХГФИЖ ЗКОЦЖСУРОЧЕ СЧ**». Уже на этом простом примере видно, что такой шифр намного сложнее, чем использованный на прошлой неделе.

Шифрограмму, полученную описанным методом, необходимо вставить во второе письмо для юного криптоаналитика. Соответственно, можно написать что-то открытым текстом, а в него вставить подготовленную шифрограмму. Письмо отправляется обычным порядком. Скорее всего, ребёнок испытает определённые сложности с расшифровкой послания, поскольку это дело достаточно трудоёмкое, так что рекомендую сразу готовиться к тому, чтобы объяснить ребёнку суть метода, способ шифрования и дешифровки, а также совместными усилиями дешифровать полученную шифрограмму.

Неделя 3. Стеганография и код Фрэнсиса Бэкона

Теперь предлагаю изучить один очень занятный метод стеганографии (и криптографии одновременно). Этот метод переворачивает сознание у тех, кто впервые о нём узнаёт, хотя, по сути, он очень прост. Но переворот сознания необходим тем, кто старается познать тайны криптографии, поэтому мы должны рассмотреть этот метод.

Что такое стеганография? Это набор методов и практик сокрытия сообщений. Основная цель стеганографии заключается в том, чтобы скрыть сам факт передачи тайного сообщения. Другими словами, тайное сообщение как бы прячется. Оно даже может быть не шифрованным. Но если спрятанное сообщение ещё и зашифровать каким-нибудь способом, то степень защиты будет повышена, особенно если метод шифрования нарушает частоты распределения символов в шифруемом тексте. Тогда найти стеганограмму намного сложнее, поскольку она начинает выглядеть как «шум». Непосвящённый человек не сможет выявить её, а у криптоаналитика будет очень мало зацепок, чтобы попытаться обнаружить стеганограмму (например, статистическими методами).

В течение третьей недели мы научимся скрывать сообщение методом, который придумал английский философ и математик Фрэнсис Бэкон. Мы немного изменим его метод и

применим его для русского языка. В итоге получится очень интересная вещь, которой можно пользоваться в любых областях жизни. Начнём же…

Помните, я не зря упомянул о том, что в нашем новом алфавите *ровно* тридцать два символа. Число 32 для криптографов и математиков – «круглое», поскольку в двоичной системе счисления записывается как «100000». Другими словами, для представления тридцати двух символов нам требуется 5 бит информации, поскольку $32 = 2^5$. Мы можем воспользоваться этим для нового способа кодирования символов нашего алфавита:

ПРОБЕЛ	00000	**З**	01000	**П**	10000	**Ч**	11000
А	00001	**И**	01001	**Р**	10001	**Ш**	11001
Б	00010	**Й**	01010	**С**	10010	**Щ**	11010
В	00011	**К**	01011	**Т**	10011	**Ъ**	11011
Г	00100	**Л**	01100	**У**	10100	**Ы**	11100
Д	00101	**М**	01101	**Ф**	10101	**Э**	11101
Е	00110	**Н**	01110	**Х**	10110	**Ю**	11110
Ж	00111	**О**	01111	**Ц**	10111	**Я**	11111

Тот из читателей, кто изощрён в информатике или программировании, уже понял, что это двоичный код для всех тридцати двух символов. Другими словами, каждому символу из алфавита ставится в соответствие пятизначное двоичное число, то есть число, состоящее ровно из пяти цифр 0 или 1. При этом нули на первых местах не удаляются, как мы это привыкли делать в десятичной системе. Здесь особенно важно, чтобы длина кода для каждого символа была равна пяти.

Соответственно, чтобы зашифровать текст, необходимо выписать один за другим код каждого символа. Например, пусть есть текст «ПОДГОТОВЬ ИНГРЕДИЕНТЫ К МОЕМУ ПРИЕЗДУ». Этот текст шифруется при помощи представленного выше кода так:

100000111100101001000111110011011110001111011000000100101110001001000100110001010100100110011101001111100000000101100000011010111100110011011010000000100001000101001001100100000010110100

А тепер**ь сам**ое **гла**вн**о**е. П**устьц**иф**ра** 0 **обо**знач**аето**б**ыч**ную бук**в**у, **а** ц**ифр**а 1 – **ж**ир**н**ую. **Весь**этот **код** м**о**жн**о** «н**анести»** н**а** пр**оизво**льный тек**с**т **пр**и помощ**итак**о**госо**от**ве**тст**вия.** И, самое гл**а**вное, нео**бяза**т**е**ль**но** ис**п**ользо**вать св**ойство жирности символа, для этих целей подойдёт любое двоичное свойство: большая буква или маленькая буква, прямая или курсив, красного цвета или чёрного. Можно даже использовать такие свойства, как «находится в первой половине алфавита или во второй» или «находится на чётном месте в алфавите или на нечётном». Но эти два последних свойства сложнее, при помощи их спрятать код можно не в любом тексте.

Как видно, эта же шифрограмма «нанесена» на обычные слова в начале предыдущего абзаца, при этом использовались все символы для нанесения (то есть и цифры, и знаки препинания). Неподготовленный читатель даже не обратит внимания на такое странное начертание текста. Но грамотный криптоаналитик, конечно же, всё сразу поймёт, этим никого не удивишь. Поэтому обычно используют более тонкие свойства, которые не так тривиальны и не видны невооружённым глазом.

Таким образом, на третьей неделе обучения надо составить и написать письмо, шифрограмма в котором будет скрыта. При составлении текста, подлежащего сокрытию, необходимо иметь в виду, что для его кодирования с помощью жирных начертаний требуется в пять раз больше символов. Я рекомендовал бы написать обычное письмо, в тексте которого не ведётся речь о шифровании вообще. А вот в скрываемом тексте можно использовать какие-нибудь нравоучения на тему, как хорошо знать и уметь заниматься шифрованием и дешифровкой.

Необходимо быть крайне внимательным при кодировании текста. Нет ничего страшного в том, что в каком-нибудь одном месте будет изменён один бит (0 на 1 или 1 на 0), поскольку это всего лишь приведёт к появлению единичной ошибки в дешифрованном открытом тексте. Намного хуже будет, если в какой-то момент будет пропущен бит. Это приведёт к сдвигу, в результате которого после расшифровки получится бессмыслица. Нет, в конце концов, её тоже можно будет расшифровать, поскольку это будет довольно структурированная бессмыслица. Но её вид вызовет у ребёнка недоумение, поскольку он подумает, что идёт по неправильному пути.

Поэтому я рекомендую воспользоваться компьютером, чтобы подготовить и затем проверить кодирование скрытого текста. Затем можно будет перенести его в письмо, которое, как мы договорились, лучше писать от руки. Соответственно, при кодировании скрытого текста надо внимательно относиться к жирности букв, поскольку для образовательных целей нужно, чтобы два состояния символов отличались друг от друга.

Неделя 4. Операция XOR

Четвёртая неделя знаменуется изучением важнейшей для криптографии математической операции, которая называется «Исключающее ИЛИ» и обозначается символом «$\oplus$». Эта операция работает на битах: на вход она принимает два бита, а возвращает один. В результате получается значение 0 тогда, когда оба входных бита одинаковы, и 1, когда входные биты различны. Другими словами, таблица истинности этой операции выглядит следующим образом:

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

Эта операция обладает одним важным свойством. Если повторно применить эту операцию с тем же самым вторым операндом к одному биту, то в результате вернется первоначальное значение этого бита. Другими словами: $(x \oplus y) \oplus y = x$ Это свойство вытекает из ассоциативности операции и того наблюдения, что её применение к двум одинаковым значениям всегда возвращает 0, каким бы ни были эти значения, а если применить эту операцию с некоторым битом и нулём, то в результате получится этот бит. То есть: $(x \oplus y) \oplus y = x \oplus (y \oplus y) = x \oplus 0 = x$.

Как происходит использование этой операции в шифровании? Пусть x – бит открытого текста, а y – бит ключа. Тогда $z = (x \oplus y)$ – это бит шифрограммы. Как же теперь расшифровать шифрограмму и получить обратно открытый текст? Абсолютно также: $x = (z \oplus y)$, то есть повторно применить ключ к шифрограмме. Это крайне удобно, поскольку для шифрования и расшифровывания нужна одна и та же операция.

Теперь давайте вспомним способ кодирования, который мы ввели на прошлой неделе. Каждая буква открытого текста была представлена пятью символами 0 и 1, то есть пятью битами. Что интересно, операцию «Исключающее ИЛИ» можно производить побитно, её можно даже применять «в столбик»:

$$\begin{array}{r} 01001 \\ \underline{10110} \\ 11111 \end{array}$$

Другими словами, побитное применение операции обозначает, что мы можем применять её к каждому биту, не обращая внимания на остальные, и результат всё равно будет правильным. Здесь нет переносов между разрядами, как при умножении или сложении. Каждая битовая позиция отвечает сама за себя.

Это даёт очень простой способ шифрования текста. Если при помощи двоичного кода перевести открытое сообщение в последовательность нулей и единиц, а потом побитно применить операцию «Исключающее ИЛИ» к этому длинному числу вместе с циклическим ключом, то получится ещё одно длинное двоичное число. Это число можно всё так же перевести назад в буквы, и это получится не что иное, как многоалфавитная замена. Впрочем, ключ можно сделать произвольной длины, в том числе и не кратной числу 5, тогда количество алфавитов в многоалфавитной замене сильно увеличится. Сейчас мы узнали ещё один, причём довольно простой, метод делать то, что мы уже умеем. При этом уже нет никакого резона заниматься арифметикой вычетов или использовать огромную таблицу.

Например, пусть надо закодировать фразу «ЖДИ СИГНАЛ ВО ВТОРНИК» при помощи ключа «ОГОНЬ». В этом случае надо взять и выписать одно под другим два больших числа, а потом применить к ним операцию «Исключающее ИЛИ»:

$$\begin{array}{r} 00111001010100100000100100100100100 \\ \underline{01111001000111101110110110111100100} \\ 01000000010011001110010010011000000 \end{array}$$

$$\begin{array}{r} 01110000010110000000000110111100000 \\ \underline{01111011101101101111001000111101110} \\ 00001011111011101111001110000001110 \end{array}$$

$$\begin{array}{r} 00011100110111110001011100100101011 \\ \underline{11011011110010001111011101101101111} \\ 11000111000101111110000001001000100 \end{array}$$

В итоге получается такая шифрограмма: «ЗАЕНИЕ АОЦОЖ НЧЫКЮ СГ». Её и можно скрывать в тексте при помощи метода стеганографии, описанном для занятий на прошлой неделе.

Однако для занятий с ребёнком на этой неделе я рекомендую использовать ключ длиной в 1 символ. Суть в том, что сейчас юному криптографу важнее научиться использовать операцию «Исключающее ИЛИ», чем заниматься расшифровыванием шифрограммы, закодированной при помощи многоалфавитной подстановки (это всё-таки довольно сложно делать вручную; и мы этим уже занимались на второй неделе).

Итак, что нужно сделать:

1. Придумать сообщение длиной не более 100 символов, которое подвергнется зашифровыванию и сокрытию.

2. Выбрать число от 1 до 31. Это будет ключ.

3. Перевести придуманное сообщение в двоичный код и применить к нему ключ.

4. Написать письмо и в одном из абзацев спрятать стеганограмму методом, изученным на прошлой неделе.

5. В самом тексте письма в открытом виде в каком-либо отвлечённом контексте упомянуть выбранное в качестве ключа число. Поскольку в этом упражнении ключом служит одна буква, то упомянуть можно её номер, но не в явном виде, а как-нибудь хитро (указание на дату рождения, номер дома бабушки или ещё что-то подобное; название гексаграммы из Книги Перемен, наконец).

Надо отметить, что так же, как и на второй неделе, когда мы изучали арифметику вычетов, можно заранее составить таблицу 32 × 32, в которой выписать все комбинации букв. Пользоваться ей ещё проще, чем предыдущей таблицей, поскольку она симметрична относительно главной диагонали. Кроме того, кодирование и декодирование производятся одним и тем же способом, а не разными, как в арифметике вычетов. Ведь для сложения обратным является вычитание, в то время как для операции «Исключающее ИЛИ» обратной является она же.

Неделя 5. Тарабарская грамота

Теперь познакомимся ещё с одним видом стеганографии, который в определённых случаях может оказаться настолько сложным для взлома, что иной криптоаналитик за голову схватится, но всё равно взломать не сможет. Этот способ очень сложен, поскольку информация прячется в тексте, который должен быть вполне обычным, чтобы не вызвать подозрений своей необычностью у криптоаналитика.

Представьте, что у переписывающихся лиц есть два канала передачи информации. Первый канал «абсолютно» закрыт (слово «абсолютно» взято в кавычки, потому что настоящую закрытость реализовать практически невозможно). К примеру, один из каналов – личное общение двух лиц тет-а-тет в закрытом помещении, проверенном на отсутствие прослушивающих устройств. Следовательно, эти лица могут обменяться какой-то информацией. Само собой разумеется, что при помощи такого канала лучше всего обмениваться ключами, то есть информацией о том, как расшифровывать сообщения, посылаемые по другому каналу.

Другой канал – «открытый», поскольку в нём существует риск перехвата сообщения. Отправка писем (как обычных, так и незашифрованных электронных), телефонные переговоры, печатание объявлений в газетах – это всё примеры открытых каналов.

Злоумышленник может получить доступ к передаваемой информации. Передавать секретную информацию в незашифрованном виде по открытому каналу нельзя, и именно поэтому необходим закрытый канал, чтобы договориться о способе шифрования. Потом уже, если способ шифрования достаточно сложен для взлома, можно обмениваться информацией по открытому каналу: технически это намного проще, но злоумышленник уже не сможет так просто получить секретную информацию.

Например, если мы договоримся, что в некотором тексте надо читать только каждую пятую букву, то это будет довольно серьёзный способ сокрытия. Не каждый начинающий криптоаналитик догадается, что надо сделать, чтобы найти секретное сообщение, особенно если оно короткое. В особенности, если текст, в котором считаются буквы, представляет собой связное и адекватное повествование. Если же текст неадекватен (похож, к примеру, на бессвязные творения поэтов-авангардистов), то криптоаналитик с опытом поймёт подвох и сможет, проведя статистический анализ по разным критериям, в конце концов взломать секретное сообщение. Если же сообщение представляет собой случайный набор символов (поле букв), то оно тем более будет взломано, причём намного быстрее.

Понятно, что составить текст, в котором содержится тайное сообщение, так, чтобы он был адекватным, но при этом на нужных местах были правильные буквы, очень сложно. Намного сложнее, чем скрывать смысл сообщений при помощи шифров простой алфавитной замены. Например, пусть надо спрятать сообщение «ЗАВТРА НАЧНУ» в тексте так, чтобы читать надо было каждую пятую букву. Начинаем с простого:

«____З____А____В____Т____Р____А____Н____А____Ч____Н____У*».

Теперь вместо знаков подчёркивания «_» подбираем буквы так, чтобы они составили вполне обычный текст, который не должен вызвать подозрения у криптоаналитика. Это сродни составлению кроссвордов.

Например, это может быть что-то такое: «У НЕЁ **З**АВТР**А**К БЫЛ **В** ДЕВЯ**Т**Ь. ТАК **Р**АНО С**А**МОЙ И **Н**АГОЙ **А**ННЕ О**Ч**КИ НЕ **Н**УЖНЫ. **У**ШЛА». Как видно, текст странный, так письма не пишут. Поэтому, как говорилось ранее, составить нормальный текст затруднительно.

А можно пойти другим путём. Например, таким способом можно записать несколько сообщений, в том числе противоречащих друг другу, перемешав их буквы. Например, вот текст: «ЗСПСП АЕРПР ВГИАИ ТОДСВ РДУИЕ АНЗБЗ НЯАОИ АУВТМ ЧЕТЕЯ НДРБС УУАЕО». Если выписать эти пятибуквенные сочетания одно под другим в столбик, то в пяти столбцах можно будет прочитать пять разных посланий. Но какое из них нужное? Впрочем, получив эти расшифровки, криптоаналитик может учесть содержание каждой, так что такой способ сокрытия тайн тоже не очень хорош.

В общем, тут есть огромные возможности для экспериментов и изысканий. Главное – как было написано в начале этого раздела, необходимо договориться о способе передачи тайной информации.

Наконец, можно рассказать ещё об одном методе, самом простом в рассматриваемом классе. По его наименованию можно назвать всю группу – «Тарабарская грамота». Им мы на этой неделе и займёмся. Суть этого метода заключается в том, что сообщение прячется среди символов из других алфавитов. При этом читать надо только буквы русского гражданского письма, а остальные игнорировать. Примерно вот так: «ZCIWEГ QUOLNД FIHUЯ DUПROD EQДLESM HRAQUSL ДREJUЛON». Тут буквы кириллицы перемешаны с буквами латиницы. Вычёркиваем из этого текста все латинские буквы, которых нет в русском языке, и получаем открытый текст.

Тут можно использовать такой нюанс. В латинском и русском алфавитах есть набор символов, которые совпадают по начертанию. Это следующие символы: A B C E H K M O P T X Y (12 символов). Что, если составить открытое сообщение только из этих символов? Это сложно, но возможно. Вот несколько примеров слов, которые можно из них составить: BECHA, POT, ABTOXTOH, MOPE, MOPEHA, TOPT, KAMOPKA, KYPOPT и т. д. Можно составить огромное количество таких слов. Вероятно, можно составить и тайное послание. Тогда эти слова можно спрятать среди латинских букв. Тогда у криптоаналитика возникнет меньше подозрений, чем если он будет смотреть на предыдущий текст, в котором были перемешаны символы латиницы и кириллицы. Также можно придумать систему кодирования из двух таких символов, и при помощи таких пар кодировать все буквы русского алфавита.

То же самое можно сделать и с греческим алфавитом, который более похож на кириллицу. Вот совпадающие символы: Α Β Γ Ε Η Κ Λ Μ Ο Π Ρ Τ Φ Χ (14 символов). С ними можно поступить абсолютно так же, как и с латиницей.

Возьмём латиницу (все знают латиницу, лишь немногие знают греческий алфавит). Закодируем тайное послание при помощи упомянутых двенадцати символов. Затем подберём слова на английском языке, в которых содержатся эти символы, но только те, что нам нужны. Подобрать такие слова намного легче, нежели решать задачу, с которой мы боролись ранее. Например, давайте попробуем закодировать то же самое послание «ЗАВТРА НАЧНУ». Пусть код выглядит следующим образом (снова воспользуемся алфавитом из тридцати двух символов для единообразия):

ПРОБЕЛ	AB	З	EB	П	OB	Ч	YB
А	AC	И	EC	Р	OC	Ш	YC
Б	AH	Й	EH	С	OH	Щ	YH
В	AK	К	EK	Т	OK	Ъ	YK
Г	AM	Л	EM	У	OM	Ы	YM
Д	AP	М	EP	Ф	OP	Э	YP
Е	AT	Н	ET	Х	OT	Ю	YT
Ж	AX	О	EX	Ц	OX	Я	YX

Внезапно оказалось кстати, что $32 = 4 \times 8$, а $12 = 4 + 8$, и среди этих двенадцати символов 4 гласных и 8 согласных. Поэтому код получился очень забавным – это двухбуквенный код, где на первом месте стоит гласная, а на втором согласная буква. Гласная буква определяет номер четвёрки (то есть столбец, в котором записана шифруемая буква), а согласная – позицию внутри четвёрки. Всё очень логично. Кстати, хоть это и красиво, но сразу же снижает ценность кода, поскольку любая регулярность даёт криптоаналитику подсказки для взлома. Но сейчас мы воспользуемся именно таким методом.

Итак, наше послание

«ЗАВТРА НАЧНУ»

перекодируется при помощи созданного кода в такую последовательность:

«EBACAKOKOCACABETACYBETOM».

Здесь 24 символа латинского алфавита, из которых надо составить список английский слов. Например, вот так:

ZEBRA CAN KOFF KLON CAR UCLA BETA CYBER TIRO MUZZ

Опять же, не очень-то складно (вообще нескладно), но это свойство всех подобных способов сокрытия информации.

Итак, на текущей неделе необходимо сделать следующее:

1. Придумать короткое сообщение, которое будет скрыто в тарабарской грамоте.

2. Закодировать его при помощи приведённой выше таблицы.

3. Придумать англоязычный текст, в котором будет скрыто сообщение.

4. Написать обычное письмо своему ребёнку, а в качестве одного из абзацев привести сгенерированный на предыдущем шаге текст на английском языке. Хорошо, если само письмо будет как-то обыгрывать эту вставку английского текста.

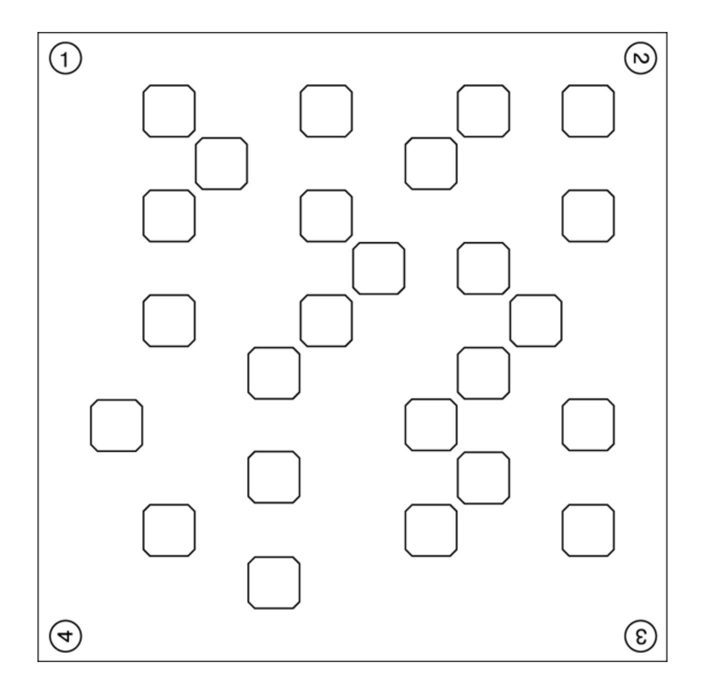
5. Далее, надо быть готовым помочь ребёнку с расшифровкой, поскольку у него могут возникнуть затруднения, особенно если ещё не совсем хорошо знает латинский алфавит.

Кстати, задачка для вдумчивого читателя и неназойливых размышлений на досуге. Конечно же, для английского языка тоже есть таблица частоты проявления символов. Можно составить новую таблицу двухбуквенной кодировки при помощи двенадцати символов, в которой будут учтены частоты встречаемости букв как в русском, так и в английском языке. Например, буква «E» встречается в английском языке чаще всего, за ней на втором месте стоит буква «T», так что резонно код «ET» отдать пробелу. А вот буква «X» встречается очень редко, равно как и буква «Y», так что код «YX» отдаётся букве «Ъ». И так далее.

Неделя 6. Шифрование дырявой матрицей

На шестой неделе мы научим ребёнка использовать так называемую «дырявую матрицу», чтобы шифровать свои тексты. Этот метод относится к перестановочным шифрам, то есть он не заменяет символы, а перемешивает их. Это, в свою очередь, значит, что частоты символов не меняются, а секретность основана на отсутствии у третьих лиц информации о точном способе перемешивания символов. И чем больше символов перемешивается, тем труднее разгадать тайну.

Для такого шифрования необходимо подготовить набор ключей. Каждый ключ представляет собой квадратную матрицу, в которой прорезаны отверстия. Другими словами, ключ – это квадратный лист картона, разделённый на знакоместа. В нем продырявлена ровно четверть знакомест. При этом отверстия сделаны таким образом, что при повороте квадрата на 90, 180 и 270 градусов их наложения друг на друга не происходит. Например, вот изображение ключа для перемешивания сообщения из 100 символов:



Как видно, это квадратный ключ. Цифрами в уголках обозначена последовательность, в которой углы ключа занимают верхний левый угол.

В прорезях пишется текст, который надо перемешать. Как только первые 25 символов текста записаны, ключ поворачивается на 90 градусов так, чтобы в верхнем левом углу теперь стояла цифра 2, и в прорези записываются следующие 25 символов перемешиваемого текста – и так далее до окончательного заполнения матрицы. Если в перемешиваемом тексте менее 100 символов, то остаток заполняется какой-нибудь буквой (например, наиболее часто используемой; но лучше подобрать сообщение так, чтобы в конце оставалось как можно меньше неиспользованных знакомест: заполнение их символами-пустышками повышает риск раскрытия – поразмыслите, почему так).

Самое важное в квадратном ключе заключается в том, чтобы при его повороте на 90, 180 и 270 градусов отверстия ни разу не совпадали. Вам необходимо будет потренироваться в создании таких ключей (кто-нибудь из читателей, умудрённых в математике, может составить систему уравнений и решить её; иной читатель, умудрённый в программировании, разработает программу для генерации подобных матриц). При этом желательно, чтобы отверстия были равномерно распределены по площади ключа, поскольку слишком отчётливые группировки опять снижают криптостойкость. Лучше всего сделать ключ, похожий на изображенный выше – отверстия не должны соприкасаться сторонами друг с другом. Понятно, что длина стороны такого ключа должна быть чётным числом.

Вот, что необходимо сделать на этой неделе:

1. Разработать свой вариант ключа размером не менее 10 × 10 для перемешивания сообщения из 100 символов.

2. Нарисовать разработанный ключ в каком-либо графическом редакторе (что-то типа MS Visio).

3. Распечатать ключ в двух экземплярах, заламинировать их оба при помощи скотча, а затем в скотче прорезать отверстия. Всё это надо сделать очень аккуратно.

4. Подготовить шифрограмму длиной не более 100 символов (лучше ровно 100, но точно не менее 90).

5. Как обычно, написать письмо юному криптоаналитику, в котором привести подготовленную шифрограмму. В письме не должно быть инструкций о том, как использовать ключ.

6. Отправить письмо, вложив в него один экземпляр ключа.

Ребёнок должен будет самостоятельно догадаться, как использовать ключ. Это упражнение призвано пробудить в нём желание сделать собственный ключ (или даже несколько ключей).

Неделя 7. Древние и кзотические алфавиты

На этой неделе мы немного отвлечёмся от основной темы и познакомимся с системами письменности, которые придумало человечество за свою историю. Во-первых, это поможет ребёнку изучить что-то новое и иногда блистать знаниями в подходящих случаях. А во-вторых, тема этой недели позволит ребёнку немного передохнуть. Мы как раз прошли половину пути, и, действительно, надо сделать небольшую передышку.

Изучение древних и экзотических алфавитов интересно ещё и потому, что некоторые не очень опытные шифровальщики могут использовать такие алфавиты для засекречивания своих посланий. Если вы видите письмо, отправленное русским другому русскому, но написанное, например, при помощи деванагари, то первое, что можно сделать, это попытаться прочитать эти буквы письменности так, как это сделал бы индус. Возможно, что в результате такого прочтения проявятся именно русские слова, а не хинди или санскрит. В истории такое происходило не раз, в этом нет ничего удивительного.

Люди за свою историю изобрели огромное количество алфавитов и неалфавитных систем письма, которые использовались (и используются) для записи как существующих языков, так и искусственных, используемых только любителями. Далее я кратко охарактеризую системы письма без самих таблиц символов, поскольку считаю, что читатель, взявшийся за этот вопрос, самостоятельно может найти всю необходимую информацию в сторонних источниках.

На заре своего развития человек пользовался так называемыми пиктографической и идеографической системами письма, в которых смысл передавался при помощи рисунков, довольно натуралистично или же схематично отражающих содержание послания. Использование этих систем было очень непростым, поскольку можно было передать лишь общий смысл того, что задумал автор надписи, да и то не всегда. Затем постепенно формировались первые системы письменности – зачатки тех, какие мы знаем сегодня.

После пиктографического письма стало появляться письмо иероглифическое. Причина его появления, скорее всего, в том, что людям нужно было упростить запись текстов и передавать знания о письме друг другу (обучение). Так что в иероглифическом письме постепенно появлялись типичные конструктивные элементы, повторяющиеся в разных знаках. Однако такое письмо сохраняло существенный недостаток своего предшественника: поскольку знаки были оторваны от звучания слова, письменная и устная речь существовали как бы по отдельности. А если в языке формы слов изменяются в зависимости от синтаксической роли, то к иероглифическим знакам приходилось добавлять большое количество модификаторов, обозначающих синтаксические отношения между словами.

Следующим шагом было использование слогового письма, когда один символ обозначал слог. Сегодня на Земле только в нескольких языках до сих пор используется этот тип письма (японский язык, большинство языков Индии, и даже в китайском языке «иероглифы» обозначают слоги). Тут может быть два варианта. Первый – в слоговом письме записываются только согласные слова, а гласные либо не записываются вовсе, либо для их обозначения применяются различные модифицирующие значки (диакритики). В основном таким методом

пользуются семитские языки, в которых такой тип письма обусловлен также спецификой морфологии и словообразования. Второй вариант – это использование различных знаков для всего многообразия слогов в языке. По этому пути пошёл японский язык и многие другие азиатские языки (в том числе и китайский).

Наконец, вершиной развития письменной речи стало появление алфавитного письма, в котором отдельные знаки обозначали в основном фонемы или аллофоны: как согласные, так и гласные звуки. Этот вид письменности, похоже, впервые был использован в Древней Греции, когда стало понятно, что заимствованное финикийское (слоговое) письмо не слишком подходит для передачи изменяющихся греческих слов, в которых изменения часто затрагивали гласные звуки. Тогда древние греки ввели в свой алфавит специальные знаки для обозначения гласных звуков. Затем из греческого письма развились кириллица и латиница (и ещё несколько других, реже используемых систем письменности), и алфавитное письмо победно зашагало по миру.

Что же нужно будет сделать на этой неделе, чтобы дать ребёнку представление о различных алфавитах? Предлагаю следующий план:

1. Составить текст письма, которое будет отправлено ребёнку.

2. Выбрать три или четыре системы письма из числа слоговых и (или) алфавитных. Предлагаю на выбор: армянское письмо, германские руны, греческое письмо, грузинское письмо, деванагари, еврейское письмо, огамическое письмо, орхоно-енисейское письмо, японское письмо (либо катакана, либо хирагана).

3. Для выбранных систем письменности составить прямые соответствия с буквами русского алфавита. Для тех букв русского алфавита, для которых нет соответствия, необходимо составить буквосочетания таким образом, чтобы можно было сделать однозначное сопоставление (вроде буквосочетаний CH, SH и т. д. в английском языке).

4. Записать при помощи выбранных алфавитных систем составленное письмо и отправить его.

Юному криптоаналитику нужно будет расшифровать полученное сообщение при помощи таблиц соответствия иноязычных символов буквам русской азбуки. Это упражнение поможет ему изучить системы письменности разных народов и культур мира.

Неделя 8. Шифрование на основе редкой книги

Следующий вид шифрования, который мы изучим, основан на использовании на выборе букв из какого-либо текста. Ведь буквы одинаковы во всех текстах, независимо от их смысла, и можно использовать произвольную последовательность символов так, чтобы кодировать и зашифровывать свои тайные послания. Такой метод шифрования достаточно стоек к взлому. А выбранный текст, естественно, становится ключом, который надо хранить в секрете.

Здесь снова идёт речь о двойном канале передачи информации. По секретному каналу происходит обмен ключей (один раз), а затем по открытому каналу пересылаются зашифрованные сообщения. Таким образом, задача в этом случае следующая: секретная передача корреспонденту какой-либо книги и разъяснение метода шифрования.

Итак, представьте себе, что получена шифровка, в которой хотя и довольно большое количество знаков, но ни один «символ» не повторяется. Под словом «символ» здесь имеется в виду некая последовательность цифр, которая обозначает одну букву. Как можно

расшифровать последовательность таких символов, если их нельзя подвергнуть частотному анализу и в них практически невозможно найти какой-либо закономерности? Кажется, это просто «белый шум», в котором невозможно отыскать что-то, за что можно зацепиться.

Организовать такую передачу очень несложно. Поговаривают, что этим способом пользовались советские разведчики и агенты, выполнявшие задания за рубежом. И у спецслужб тех государств, против которых велась работа, опускались руки, поскольку расшифровать подобное можно, только если каким-то образом получить ключ. А получить ключ – значит выдать себя, дать понять другой стороне, что ведётся работа по дешифровке. В этом случае уже используются совсем иные методы, и о некоторых из них даже страшно упоминать в такой книге, как эта. Но как только попытка дешифровки стала явной для стороны, которая шифрует свои послания, она тут же меняет ключ, и всё возвращается на исходные позиции.

Тем не менее то, что мы изучим на этой неделе, – простой и надёжный метод шифрования (при условии сохранности ключа). Для занятий необходимо подобрать какую-либо книгу, достаточно редкую, чтобы её было невозможно найти на каждом углу. Пусть книга будет потолще, чтобы хватило надолго. Требуются два экземпляра этой книги, поскольку она будет ключом. Как уже сказано, ключом необходимо обменяться по тайному каналу, так что после обмена у каждой из сторон переписки будет по одному экземпляру книги.

Шифрование производится следующим образом. Каждая буква обозначается тройкой чисел (номер страницы, номер строки, номер буквы). Можно прямо так и записывать в скобках:

(5 17 23) (7 24 6) (3 3 17) (3 14 25) (10 15 18) (8 5 25)

Теперь понятно, почему ни один символ в шифровке не повторится никогда. В любой книге намного-намного больше букв, чем в шифрованном сообщении, которое оперативно передаётся между двумя людьми. Можно выбирать буквы в книге так, чтобы их «координаты» никогда не повторялись. Для этого надо сразу же вычёркивать те буквы, которые были использованы. Так будет обеспечено однократное использование любой буквы из книги, а это станет гарантией того, что шифр не будет взломан. Единственная проблема – книга с вычеркнутыми буквами всегда наводит криптоаналитика на определённые размышления. Если у криптоаналитика появился доступ к книгам, хранящимся у тех, кто ведёт переписку, то тайна через некоторое время тайной быть перестанет.

Соответственно, расшифровка производится таким же образом. При расшифровке тоже надо вычёркивать встретившиеся буквы, чтобы не использовать их при шифровании ответных посланий. В результате получается очень секретный способ передачи информации.

Для занятий на этой неделе необходимо:

1. Подобрать два экземпляра одной достаточно редкой книги. Один оставить у себя, второй отправить ребёнку. Желательно отправить книгу заранее (ещё лучше – в самом начале занятий, но не говорить, для чего эта книга).

2. Составить письмо, которое будет отправлено юному криптографу.

3. В письмо вставить послание, зашифрованное методом, описанным выше.

4. Если у ребёнка возникнут затруднения в расшифровке, то быть готовым ему помочь.

Если ребёнок достаточно проницателен, он сможет и без подсказок понять, для чего он взял с собой книгу, особенно если эта книга не предназначена для летнего чтения.

Неделя 9. Замена целых понятий

Теперь пришло время обучить юного криптографа ещё одному методу сокрытия информации, который в криптографии часто называется «кодированием». В этом варианте специальные коды используются для шифрования отдельных понятий.

Прежде чем углубиться в этот метод подробно, необходимо изучить понятие «знак». По определению знаком называется *соглашение* о приписывании чему-либо (означающему) какого-либо определённого смысла или значения (означаемого). Например, буквы, которые вы сейчас читаете, являются знаками для обозначения звуков русского языка. А слова, которые состоят из букв, являются знаками для обозначения смысла речи. Цифры – это знаки для обозначения чисел. В математике, в программировании используется огромное количество знаков. Или, к примеру, дорожные знаки обозначают те или иные понятия из области дорожного движения.

Главное в этом определении – слово «соглашение». Знаком будет считаться только то, о чём договорились, по крайней мере, два человека. И эта мысль даёт подсказку к тому методу сокрытия информации, который мы сейчас будем изучать. Ведь можно создать собственную систему знаков, смысл которых не будет понятен непосвящённому. То, что мы изучали на первой неделе, и есть попытка создать такую систему. Но эта попытка была негодной, поскольку в основе создаваемой системы лежали известные закономерности, так что взломать её, оказывается, совсем просто. А если сделать знаковую систему, которая не будет иметь таких откровенных закономерностей? Легко!

Например, молодые люди договариваются, что девушка будет выставлять на подоконник горшок с цветком, когда её родителей нет дома. А молодой человек, возвращаясь вечером из института, высматривает цветок на подоконнике и по его появлению понимает, как можно провести вечер. Это явный знак, смысл которого вполне понятен влюблённой паре. Они договорились о смыслах, которые будут нести наличие и отсутствие цветка, и это стало знаком для них. Посторонние смогут распознать это после длительных наблюдений за их поведением.

Или знаменитый пример, когда кодовое слово «Над всей Испанией безоблачное небо» стало сигналом для начала военного мятежа на всей территории страны. Даже если этот пароль и легенда, то он всё равно показывает, что известные посвящённым кодовые слова могут служить для синхронизации действий, то есть быть знаками.

Самое важное в деле разработки системы кодовых знаков – невозможность догадаться (или хотя бы даже предположить) о значении кода из контекста. Эту ошибку допускают многие начинающие криптографы и кодировщики, которые используют не отвлечённые понятия или случайные наборы символов, а что-то похожее на обозначаемое.

Например, глупо кодировать главнокомандующего такими словами, как «бугор», «туз» или «атаман», это будет понятно сразу же. А если использовать код «одуванчик», то криптоаналитику надо будет приложить усилия, чтобы понять, что это слово обозначает. Фраза «Одуванчик распустился поутру» может обозначать сигнал к началу атаки, а «Одуванчик опушился семенами» – сигнал к укреплению района дислокации.

Или, например, два человека договорились, что один другому пришлёт по электронной почте анекдот. Если это будет анекдот про папу римского, то такое письмо обозначает, что отправитель нашёл на дне океана затопленный испанский галеон с кучей золота на борту. А анекдот про раввина из Праги будет свидетельствовать, что поиски не привели к успеху. И подобных примеров можно привести нескончаемое количество.

Таким образом, опять видна необходимость тайной договорённости о системе кодирования ключевых понятий. Сначала нужно составить словарь в двух экземплярах, а затем по открытым каналам уже можно пересылать информацию, закодированную при помощи этого словаря.

Что обычно кодируют этим методом? Ответ простой: ключевые понятия, которые используются теми, кто занимается секретной перепиской. Это могут быть имена людей, названия населённых пунктов и мест, а также определённые действия, информацию о которых необходимо скрыть. Так что на этой неделе план работ должен быть следующим:

1. Составить словарь кодовых обозначений и передать его юному криптографу при помощи секретного канала.

2. Написать письмо, в котором все термины, встречающиеся в словаре, заменены на коды.

Опять же, словарь желательно составить до начала обучения, и передать его ребёнку тоже необходимо заранее. Иначе секретность канала его передачи окажется под сомнением, поскольку любое лицо, передавшее словарь (если это, конечно, не сам читатель), сможет его скомпрометировать.

Неделя 10. Симпатические чернила

На этой неделе мы займёмся очень интересным шпионским делом, которое наверняка привлечёт внимание юного криптографа. Это ещё один метод стеганографии, то есть сокрытия самого факта передачи информации. Речь пойдёт о так называемых симпатических чернилах, то есть таких, которые не видны невооружённым глазом, а проявляются только при определённых условиях. Такими условиями могут выступать нагрев, освещение специальным светом или использование химического проявителя. Можно сказать, что это наиболее широко используемый метод стеганографии – на листе бумаги симпатическими чернилами пишется секретный текст, а поверх него при помощи обычных чернил пишут ничего не значащее сообщение для отвода глаз.

В качестве симпатических чернил можно использовать различных вещества. Самое банальное – это обычное молоко. Если написать текст молоком, то, когда оно высохнет, видно его не будет. Проявить скрытый текст можно только нагрев лист. При нагреве написанные молоком буквы станут коричневыми. Тем же самым свойством обладают следующие вещества: яблочный сок, сок лука, сок брюквы, квасцы и даже свежая светлая моча (некоторые арестанты пользуются этим способом за неимением иных).

Также можно использовать слюну – для неё проявителем служит очень слабый водный раствор чернил. Другие вещества, которые могут использоваться в качестве симпатических чернил, – крахмал (проявлять надо при помощи йодной настойки) и аспирин (проявляется солями железа). А интересней всего использовать раствор стирального порошка с оптическим отбеливателем, поскольку эти симпатические чернила проявляются при помощи ультрафиолетового света.

Вот краткая таблица-памятка, в которой симпатические чернила расположены в порядке доступности как самих чернил, так и проявителя для них. Самый простой проявитель – нагрев, а наиболее доступные для нагрева симпатические чернила – молоко. Все остальные пары в этой таблице расположены сходным образом:

Чернила	Проявитель
Молоко	Нагрев
Яблочный сок	Нагрев
Сок лука	Нагрев
Сок брюквы	Нагрев
Свежая светлая моча	Нагрев
Квасцы	Нагрев
Спиртовой раствор пирамидона	Нагрев
Стиральный порошок с оптическим отбеливателем	Ультрафиолетовый свет
Воск	Мел или зубной порошок
Слюна	Очень слабый водный раствор чернил
Пищевая лимонная кислота	Бензиловый оранжевый индикатор
Крахмал	Йодная настойка
Аспирин	Соли железа
Фенолфталеин	Разбавленная щёлочь

Таким образом, на этой неделе план обучения ребёнка следующий:

1. Выбрать симпатические чернила таким образом, чтобы у ребёнка заведомо была возможность их проявить. Лучше всего использовать молоко.

2. Написать скрытый текст выбранными симпатическими чернилами и дождаться, когда он полностью высохнет. Лучше использовать большие, размашистые буквы, чтобы при проявке они не сливались ни друг с другом, ни с символами открытого текста.

3. Поверх текста, написанного симпатическими чернилами, написать произвольный текст на отвлеченную тему. В нём желательно как-нибудь намекнуть на то, какие симпатические чернила были использованы.

Так что на этой неделе юный криптограф научится очень интересному способу сокрытия информации, который наверняка ему понравится. По возвращении домой ему можно будет рассказать про другие варианты симпатических чернил и научить самостоятельно их готовить и проявлять.

Неделя 11. Каскадное шифрование

К одиннадцатой неделе ваш ребёнок, занимающийся криптографией, уже должен знать достаточное количество методов сокрытия информации, а также уметь использовать их для расшифровывания. Кроме того, он должен знать и уметь применять на практике изученные методы дешифровки. Мы воспользуемся этим для закрепления полученных навыков перед тем, как перейти к изучению абсолютно невзламываемого шифра.

На этой неделе мы изучим так называемое каскадное шифрование, когда для сокрытия информации используется несколько разных методов шифрования и стеганографии. Это как заворачивание предмета в несколько разных обёрток или сборка матрешки. Или как луковая шелуха – снимаешь один слой, а под ним другой. В общем, каскадное шифрование – это когда к тексту последовательно применяется несколько способов шифрования и сокрытия информации. Сначала один, потом – к полученной шифрограмме – второй, потом третий и т. д.

В чём идея? Дело в том, что информация имеет свойство устаревать. Особенно это касается оперативной информации. Например, некто переслал шифрованную команду начать атаку на окружённую крепость завтра утром. Пусть противник перехватит шифрограмму, но если он расшифрует её только к полудню завтрашнего дня, эта информация ему никак не поможет, так как атака к тому времени уже начнётся. Поэтому криптоаналитик должен действовать быстро. Но вычислительные мощности, какими бы ни были они серьёзными, всегда ограниченны, а потому тот, кто шифрует информацию, может затруднить её вскрытие на некоторое время, пока информация имеет какую-то ценность. Это, собственно, одно из предназначений каскадного шифрования.

Для каскадного шифрования можно использовать несколько достаточно простых шифров. Каждый из которых взломать, может быть, и легко – но, взломав первый, криптоаналитик наткнётся на второй. При этом надо будет ещё понять, что первый шифр взломан, а полученный на выходе хаотичный набор символов – это уже второй «слой» шифрования. После этого криптоаналитик потратит время на взлом второго шифра, а там обнаружится третий. И когда криптоаналитик, вытирая пот с поседевшей головы, найдёт открытый текст, будет уже поздно и полученная информация будет неактуальной.

Таким образом, на этой неделе необходимо выполнить следующий план работ:

1. Необходимо выбрать не менее трёх способов сокрытия информации, которые были изучены ранее. Желательно выбирать такие, в которых ребёнок «плавает», чтобы он мог дополнительно потренироваться. Но первый метод шифрования лучше выбрать как раз такой, с которым юный криптограф знаком хорошо.

2. После этого придумать текст, который будет скрыт. Соответственно, к этому тексту надо будет применить все выбранные методы шифрования и сокрытия информации.

3. Затем внести полученную шифрограмму в текст письма ребёнку.

4. В случае затруднений, ребенку надо будет помочь. Это упражнение в целом довольно-таки непростое, поэтому к дополнительной работе с ребёнком надо готовиться сразу.

Например: следует придумать сообщение длиной не менее 250 символов, после чего применить к нему шифр многоалфавитной замены с ключом длиной в 5 символов. Полученную шифрограмму закодировать методом Френсиса Бэкона (применять операцию XOR в этом случае смысла нет, так как замена, применённая к замене, даёт ту же замену, сила шифра не меняется абсолютно). Сам код Бэкона нанести на буквы открытого текста при помощи симпатических чернил (можно, к примеру, закрашивать ту букву, которая соответствует двоичной цифре 1). В итоге отправляемое письмо не будет нести никаких следов скрытой информации. Проявив симпатические чернила, ребенок получит последовательность двоичных цифр. Её надо раскодировать, но результатом окажется шифрограмма, которую снова придётся взламывать.

Таким образом, эта неделя будет для ребёнка своеобразным экзаменом. Ему потребуется применить все накопленные знания, чтобы взломать новое послание. Так что рекомендую подготовить для него какой-нибудь сюрприз и подарок.

Неделя 12. Одноразовый блокнот

Наконец, мы подошли к самой волнующей теме, которой я и хотел бы закончить эту книгу. На последней неделе занятий я познакомлю вас с абсолютно невзламываемым способом шифрования. Тексты, зашифрованные им, невозможно взломать, и это доказано математически. Способ называется «одноразовый блокнот».

Представьте себе шифрограмму, в которой текст зашифрован при помощи банальной многоалфавитной замены (напомню, что мы проходили этот метод на второй неделе и затем вновь вернулись к нему на четвёртой, когда изучали операцию XOR). Ничего сложного, правда? Но что, если длина ключа равна длине скрываемого текста, а сам ключ представляет собой абсолютно случайный набор символов? Как такое можно взломать?

Действительно, если взять абсолютно случайную последовательность символов в качестве ключа, при этом длина ключа будет равна длине шифруемого текста, то после применения операции XOR к двум последовательностям получится такой же абсолютно случайный набор символов, в котором нет никаких закономерностей. Давайте попробуем провести небольшой эксперимент.

Пусть необходимо скрыть слово «КИБЕРНЕТИКА», а в качестве ключа будем использовать последовательность «ЫУДЛДЫЯУПЛИ». Результат применения операции XOR к этим двум строкам такой: «ЦЭЖЙУСШЖШЖЗ». Как может попытаться взломать эту шифрограмму криптоаналитик? Поскольку символов здесь всего 11, он может попытаться перебрать все возможные варианты ключей (хотя это очень много даже для современных вычислительных устройств и полный перебор займёт много времени: 32^{11} = 36 028 797 018 963 968; и если пробовать миллиард комбинаций в секунду, то вся работа будет выполнена за 36 028 797 секунд, то есть примерно за полтора года). Допустим, у криптоаналитика имеется в распоряжении квантовый компьютер с достаточным количеством кубитов, тогда он сможет попробовать все 32^{11} вариантов за один раз, но что это даст?

Ничего. Пусть криптоаналитик пробует ключ «ЪУИНЦЪКУПЛИ». Тогда в результате дешифровки получится текст «ЛИНГВИСТИКА». А если криптоаналитик попробует ключ «ЗФДАЪЩЦЕЦНН», то в результате расшифровки получится текст «ЯЗЫКОЗНАНИЕ». Другими словами, после перебора всех возможных ключей длиной в 11 символов получится очень много хаотической белиберды, среди которой встретятся все, абсолютно все слова длиной в 11 букв (а также фрагменты каких-нибудь фраз длиной в 11 символов). И что должен выбрать бедный криптоаналитик? Никаких зацепок, ничего.

Тот, кто шифрует свои сообщения при помощи одноразового блокнота, должен соблюдать два несложных правила:

1. Ключ должен быть абсолютно случайным. Если в нём будут какие-либо регулярности и закономерности, это сразу даст криптоаналитику (у которого в арсенале много инструментов статистического анализа) зацепки, и в конце концов он сможет расшифровать текст.

2. Ключ никогда и ни при каких условиях не должен повторяться дважды. Никогда! Потому метод и называется «одноразовым блокнотом» – каждый ключ применяется *только* один раз. Если вы примените один и тот же ключ дважды, это будет фиаско, поскольку взломать два текста, зашифрованные одним и тем же ключом – это всё равно, что расшифровать шифр многоалфавитной замены, так как для этого используется банальный частотный анализ. Всё дело в свойстве операции XOR – как только криптоаналитик получит два разных текста, зашифрованных одним и тем же ключом, он тут же сложит их друг с другом, и неизвестный ему ключ самоуничтожится, а дальше – дело техники.

Что же такое «одноразовый блокнот»? Этот метод шифрования был придуман очень давно. Им активно пользовались во время Второй мировой войны для шифровки самых важных сообщений. Способ же шифрования был довольно незамысловатым. В двух экземплярах печатались блокноты, содержащие случайные последовательности букв. Один блокнот выдавался тайному агенту, а второй оставался в штабе. Для шифровки бралась первая страница блокнота, и символы, напечатанные на ней, использовались в качестве ключа. После шифрования страницу вырывали из блокнота и очень скрупулёзно уничтожали

(сжигали с тщательным перемешиванием и развеиванием пепла по ветру). Адресат, получивший шифрограмму, брал свою копию одноразового блокнота, расшифровывал послание при помощи текущей первой страницы, вырывал страницу и так же уничтожал её.

Этот метод был настолько надёжен, что криптоаналитики, получавшие послания, которые заведомо были зашифрованы одноразовым блокнотом, даже не пытались их расшифровывать. Впрочем, они складывали их в архив, и не зря, поскольку тайные агенты иногда ленились и шифровали послания при помощи одной и той же страницы. А иногда они не уничтожали использованные страницы, и они тем или иным способом попадали в руки криптоаналитикам. И всё.

Таким образом, вот план работ на эту неделю:

1. Придумать текст, который необходимо зашифровать.

2. Использовать для шифровки одноразовый блокнот, подготовленный с самого начала занятий. Один экземпляр блокнота должен находиться у ребёнка.

3. Вписать шифрограмму в открытый текст очередного письма.

4. Послать письмо.

5. Подготовить для юного криптографа какой-нибудь замечательный подарок в честь окончания базового курса по криптографии и значительного укрепления математических способностей.

6. Вручить подарок вернувшемуся домой ребёнку.

Это будет просто замечательно. В результате выполнения задачи ребёнок сможет на собственном опыте убедиться в абсолютной стойкости описанной системы шифрования.

Заключение

Как автор я очень надеюсь на то, что идеи и примеры, изложенные в этой книге, найдут живой отклик в сердцах моих читателей, и в итоге многие ребята и девчонки узнают о тайнах и чудесах криптографии.

Если эта тема «зацепила» ребёнка, и он хотел бы заниматься дальше, то можно посоветовать ему уже самостоятельно прочитать несколько более серьёзных книг по криптографии, которые можно найти в интернете. В книге для ребёнка я рекомендую несколько таких книг, но и здесь я также приведу несколько ссылок на довольно интересные тексты.

Далее я хочу сказать о математике. Криптография без математики состояться никак не может. Человек может уметь пользоваться криптографическими методами, но если он не понимает базовых механизмов, лежащих в их основе, то это использование будет только поверхностным, на уровне «запустить утилиту, чтобы зашифровать файл». Изучение криптографии само по себе очень развивает математические способности. Но и для того чтобы усваивать некоторые криптографические методы, необходимы хорошие математические познания и возможность быстро научиться зачастую довольно непростым вещам.

Немного об информатике. Сегодня никто уже не использует ручные методы криптографии (хотя в некоторых случаях они могут быть востребованы). Вся серьёзная криптография реализуется при помощи компьютеров, а потому владение языками программирования и алгоритмическим мышлением помогает развивать и криптографические навыки. Но, как говорил один из моих преподавателей криптографии: «Никогда не используйте свои

собственные разработки». Это из-за того, что в одиночку очень сложно продумать все возможные способы, которыми злоумышленник или криптоаналитик будет пробовать шифр на прочность. Есть примеры, когда шифр взламывался по измерению времени отклика на посылаемые запросы – по микросекундам разницы делались заключения и подбирались ключи. А разработчик, который делал эту систему шифрования, даже и помыслить не мог, что его система настолько уязвима с этой точки зрения. При этом, однако, желательно попробовать реализовать системы шифрования самостоятельно, чтобы разбираться в их внутреннем устройстве.

Продвигаясь дальше, можно подойти к теории информации. Это уже более серьёзная тема, к которой ребёнок вряд ли сможет подступиться ранее старшей школы или даже начальных курсов института. Но без теории информации криптография слаба. Это наука, лежащая в основании криптографии, так же как и математика с информатикой.

Наконец, высшим пилотажем будет постижение квантовых вычислений и теории квантовой информации. Конечно, к этим темам можно будет подступиться только после получения значительных знаний по математике, физике и кибернетике, которые обычно получают в серьёзном техническом университете. Но теория квантовой информации сейчас находится на острие науки, и в будущем это одна из самых востребованных специальностей.

Другими словами, примерная дорожная карта развития в этом направлении следующая:

1. Постоянно усиливать математические навыки ребёнка, развивать его абстрактное мышление.

2. Если он ещё не умеет, начинать учить его программированию. Советовать что-либо здесь я не могу. Возможно, что имеет смысл отдать ребёнка в какой-либо кружок по информатике.

3. Если всё пойдёт успешно, то в старшей школе можно начинать с популярных книг по кибернетике, а дальше плавно переходить к теории информации.

4. В институте, получив необходимые базовые навыки и знания, осваивать квантовые вычисления и теорию квантовой информации.

Вот так.

Если хотя бы один из тех детей, кто занимался по этой книге, добьётся успехов в области криптографии или смежных науках, то я буду считать миссию этой книги выполненной. Так что в добрый путь!

Конечно же, я жду отзывов своих читателей – присылайте их на адрес электронной почты: *roman.dushkin@gmail.com*.

Список литературы

Для лучшего развития навыков в криптографии и понимания её основ, принципов и методов я рекомендую дополнительную литературу. Этот список составлен на основе моих личных предпочтений с точки зрения интереса, художественности, подачи материала и прочих критериев. В начале списка стоят книги с наивысшей рекомендацией, а далее по убывающей.

1. **Стивенсон Н**. *Барочный цикл*. Это очень большое произведение, в котором в крайне замысловатой манере описывается история перехода Европы от Средневековья к Просвещению и становления естественнонаучного мировоззрения. Цикл очень интересный, в нём поднимается множество научно-философских вопросов. Также вспомогательными сюжетами постоянно проводятся истории о шифровании и дешифровке, и их описания дают много интересных идей.

2. **Стивенсон Н**. *Криптономикон*. Как бы продолжение «Барочного цикла», но общими остались только фамилии персонажей и наличие одного «бессмертного» героя. В этой книге рассказывается история экспоненциального развития криптографии в годы Второй мировой войны, взлом немецкой шифровальной машины «Энигма» и множество иных интересных историй из области математики, информатики и криптографии. Обязательно почитайте эту книгу.

3. **Кан Д.** *Взломщики кодов*. Популяризаторская книга о криптографии: как начиналась эта наука, как развивалась, каких успехов достигла. Рассказывается много историй о том, как взламывались те или иные системы шифрования, и в том числе о немецкой машине «Энигма».

4. **Сингх С**. *Книга шифров. Тайная история шифров и их расшифровки*. Занятная книга о криптографии, в которой приводится уйма интересных историй и познавательных описаний систем шифрования. Чтение несложное, книга популярная и простая.

5. **Жельников В.** *Криптография от папируса до компьютера*. Более или менее популярная книга для старших школьников, в которой простыми словами рассказывается история криптографии с самых древних времён и до наших дней. Приводятся описания некоторых систем криптографии.

6. **Чёрчхаус Р.** *Коды и шифры, Юлий Цезарь, «Энигма» и Интернет*. Ещё одна книга исторических очерков о криптографии – как всё начиналось и куда это привело на современном этапе развития науки. Написана достаточно легко, так что будет понятна и интересна старшеклассникам.

7. **Бауэр Ф.** *Расшифрованные секреты. Методы и принципы криптологии*. Это уже более академическая книга, в ней меньше научно-популярных слов, но больше формул. Книга должна быть интересна продвинутым криптографам и криптоаналитикам, которые постигли основы и хотят развиваться дальше. В первой её части описываются системы шифрования, а во второй – методы их взлома («атаки»).

8. **Дориченко С., Ященко В.** *25 этюдов о шифрах: Популярно о современной криптографии*. Достаточно строгая книга, в которой с использованием серьёзного математического аппарата даётся описание многих методов криптографии (как с точки зрения шифрования, так и с точки зрения дешифровки). Рекомендуется для студентов младших курсов.